



Cisco Unified Communications Manager アドミニストレーションガイド、リリース 14 および SU

初版：2022年6月16日

最終更新：2023年5月5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/>

【注意】 シスコ製品をご使用になる前に、安全上の注意（ www.cisco.com/jp/go/safety_warning/ ）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2022–2023 Cisco Systems, Inc. All rights reserved.



目次

第 1 章	新機能と更新情報 1
	新機能と更新情報 1

第 I 部 :	管理の概要 3
---------	----------------

第 2 章	管理の概要 5
	Cisco Unified CM Administration の概要 5
	オペレーティング システムの管理の概要 6
	認証済み Network Time Protocol のサポート 8
	自動キー認証済み Network Time Protocol のサポート 8
	Cisco Unified Serviceability の概要 9
	Cisco Unified Reporting の概要 10
	ディザスタ リカバリ システムの概要 11
	一括管理ツールの概要 12

第 3 章	はじめに 13
	管理インターフェイスへのログイン 13
	管理者またはセキュリティ パスワードのリセット 13
	システムのシャットダウンまたは再起動 15

第 II 部 :	ユーザの管理 17
----------	------------------

第 4 章	ユーザ アクセスの管理 19
	ユーザ アクセスの概要 19

アクセス制御グループの概要	19
ロールの概要	21
ユーザ ランクの概要	24
ユーザ アクセスの前提条件	24
ユーザ アクセスの設定タスク フロー	24
ユーザ ランク階層の設定	25
カスタム ロールの作成	26
管理者の高度なロール設定	27
アクセス制御グループの作成	28
アクセス制御グループへのユーザの割り当て	29
アクセス制御グループの重複する特権ポリシーの設定	30
ユーザ権限レポートの表示	30
カスタム ヘルプ デスク ロールの作成タスク フロー	31
カスタム ヘルプ デスク 権限の作成	31
カスタム ヘルプ デスク アクセス コントロール グループの作成	32
アクセス コントロール グループへのヘルプ デスク ロールの割り当て	32
アクセス コントロール グループへのヘルプ デスク メンバーの割り当て	33
アクセス コントロール グループの削除	34
既存の OAuth 更新トークンの取り消し	34
非アクティブなユーザ アカウントの無効化	35
リモート アカウントの設定	36
標準ロールとアクセス制御グループ	36

第 5 章**エンドユーザの管理 49**

エンドユーザの概要	49
エンドユーザ管理タスク	49
ユーザ テンプレートの設定	50
ユニバーサル回線テンプレートの設定	51
ユニバーサルデバイス テンプレートの設定	52
ユーザ プロファイルの設定	53
機能グループ テンプレートの設定	55

LDAP からのエンド ユーザのインポート	56
エンド ユーザの手動追加	57
エンド ユーザ用の新しい電話機の追加	58
エンド ユーザへの既存の電話機の移動	59
エンド ユーザ PIN の変更	60
エンド ユーザ パスワードの変更	60
Cisco Unity Connection ボイス メールボックスの作成	61

 第 6 章

アプリケーション ユーザの管理	63
アプリケーション ユーザの概要	63
アプリケーション ユーザのタスク フロー	64
新規アプリケーション ユーザの追加	64
デバイスとアプリケーション ユーザの関連付け	65
Cisco Unity または Cisco Unity Connection への管理者ユーザの追加	65
アプリケーション ユーザ パスワードの変更	67
アプリケーション ユーザ パスワード クレデンシャル情報の管理	67

 第 III 部 :

デバイスの管理 69

 第 7 章

電話の管理	71
電話管理の概要	71
電話ボタン テンプレート	71
電話機管理タスク	72
電話機の手動での追加	73
エンド ユーザの有無にかかわらずテンプレートからの新しい電話機の追加	74
エンド ユーザがあるテンプレートからの新しい電話機の追加	76
コラボレーション モバイル コンバージェンス仮想デバイスの概要	77
Collaboration モバイル コンバージェンスの仮想デバイスを追加します。	78
CMC RD 機能の相互作用	79
CMC RD 機能の制約事項	85
既存の電話機の移動	85

現在ログイン中のデバイスの検索	86
リモート ログイン デバイスの検索	87
電話機のリモート ロック	88
工場出荷時の初期状態への電話機のリセット	88
電話ロック/ワイブレポート	89
電話の LSC ステータスの表示および CAPF レポートの生成	90

第 8 章**デバイス ファームウェアの管理 93**

デバイス ファームウェアのアップデートの概要	93
デバイス パックまたは個々のファームウェアのインストール	94
ファームウェアのインストールの潜在的な問題	95
システムからの未使用のファームウェアの削除	96
電話モデルのデフォルト ファームウェアの設定	97
電話のファームウェア ロードの設定	98
ロード サーバの使用	99
非デフォルト ファームウェア ロードを使用するデバイスの検索	100

第 9 章**インフラストラクチャ デバイスの管理 101**

インフラストラクチャの管理の概要	101
インフラストラクチャの管理の前提条件	101
インフラストラクチャの管理のタスク フロー	102
インフラストラクチャ デバイスのステータスの表示	102
インフラストラクチャ デバイス トラッキングの非アクティブ化	103
非アクティブ化されたインフラストラクチャ デバイス トラッキングのアクティブ化	104

第 IV 部 :**システムの管理 105**

第 10 章**システム ステータスのモニタ 107**

クラスター ノード ステータスの表示	107
ハードウェア ステータスの表示	107
ネットワーク ステータスの表示	108

インストールされているソフトウェアの表示	108
システム ステータスの表示	109
IP 設定の表示	109
最終ログインの詳細の表示	110
ノードの ping	110
サービス パラメータの表示	111
ネットワーク DNS の設定	112

第 11 章

アラーム 115

概要	115
アラーム設定	116
アラームの定義	117
アラーム情報	118
アラームのセットアップ	119
アラーム サービスの設定	120
Syslog Agent エンタープライズ パラメータ	120
アラームサービスのセットアップ	121
Cisco Tomcat を使用するアラーム サービスのセットアップ	122
サービス グループ	123
アラーム設定	124
アラーム定義およびユーザ定義の説明の追加	129
アラーム定義の表示とユーザ定義の説明の追加	129
システム アラーム カタログの説明	130
CallManager アラーム カタログの説明	131
IM and Presence アラーム カタログの説明	132
CiscoSyslog ファイル内のデフォルトのアラーム	133

第 12 章

監査ログ 137

監査ログ	137
監査ロギング (標準)	137
監査ロギング (詳細)	142

監査ログのタイプ	142
システム監査ログ	142
アプリケーション監査ログ	143
データベース監査ログ	143
監査ログ設定タスク フロー	143
監査ロギングのセットアップ	144
リモート監査ログの転送プロトコルの設定	145
アラート通知用の電子メール サーバの設定	145
電子メールアラートの有効化	146
プラットフォーム ログのリモート監査ロギングの設定	147
監査ログの構成時の設定	148

第 13 章**Call Home 155**

Call Home	155
Smart Call Home	155
Anonymous Call Home	158
Smart Call Home による処理	160
Call Home の前提条件	162
Call Home へのアクセス	162
Call Home の設定	162
Call Home の設定	163
制限事項	166
Call Home の参照先	167

第 14 章**Serviceability Connector 169**

Serviceability Connector の概要	169
Serviceability サービスを使用する利点	170
他のハイブリッドサービスとの違い	170
動作の簡単な説明	170
TAC ケースの展開アーキテクチャ	171
Serviceability Connector の TAC サポート	173

第 15 章

簡易ネットワーク管理プロトコル 175

簡易ネットワーク管理プロトコル (SNMP) のサポート 175

SNMP の基礎 176

SNMP 管理情報ベース 177

SNMP の設定要件 194

SNMP バージョン 1 のサポート 195

SNMP バージョン 2c のサポート 195

SNMP バージョン 3 のサポート 195

SNMP サービス 196

SNMP のコミュニティストリングとユーザ 197

SNMP のトラップとインフォーム 197

SFTP サーバのサポート 199

SNMP 設定タスク フロー 200

SNMP サービスの有効化 201

SNMP コミュニティストリングの設定 202

コミュニティストリングの構成時の設定 203

SNMP ユーザの設定 205

SNMP V3 のユーザ構成時の設定 207

リモート SNMP エンジン ID の取得 209

SNMP 通知先の設定 209

SNMP V1 および V2c の通知先の設定 211

SNMP V3 の通知先の設定 213

MIB2 システム グループの設定 214

MIB2 システム グループの設定 215

CISCO-SYSLOG-MIB トラップ パラメータ 216

CISCO-CCM-MIB トラップ パラメータ 217

CISCO-UNITY-MIB トラップ パラメータ 217

SNMP Master Agent の再起動 217

SNMP トラップ設定 (SNMP Trap Settings) 218

SNMP トラップの設定 218

SNMP トラップの生成	219
SNMP トレースの設定	222
SNMP のトラブルシューティング	222

第 16 章

サービス 225

機能サービス	225
データベースおよび管理サービス	227
Locations Bandwidth Manager	227
Cisco AXL Web Service	227
Cisco UXL Web サービス	227
Cisco Bulk Provisioning サービス	227
Cisco TAPS サービス	227
Platform Administrative Web サービス	228
パフォーマンスおよびモニタリング サービス	228
Cisco Serviceability Reporter	228
Cisco CallManager SNMP サービス	228
CM サービス (CM Services)	229
Cisco CallManager	229
Cisco TFTP	229
Cisco Unified Mobile Voice Access Service	230
Cisco IP Voice Media Streaming App	230
Cisco CTIManager	230
Cisco エクステンション モビリティ	231
Cisco Dialed Number Analyzer	231
Cisco Dialed Number Analyzer Server	231
Cisco DHCP Monitor サービス	231
シスコ クラスタ間検索サービス	231
Cisco UserSync サービス	232
Cisco UserLookup Web Service	232
Cisco Headset Service	232
IM and Presence サービス	232
Cisco SIP Proxy	232

Cisco Presence Engine	232
Cisco XCP Text Conference Manager	233
Cisco XCP Web Connection Manager	233
Cisco XCP Connection Manager	233
Cisco XCP SIP Federation Connection Manager	233
Cisco XCP XMPP Federation Connection Manager	233
Cisco XCP Message Archiver	233
Cisco XCP Directory Service	233
Cisco XCP Authentication Service	233
CTI サービス	234
Cisco IP マネージャーアシスタント	234
Cisco WebDialer Web Service	234
セルフプロビジョニング IVR	234
CDR サービス	235
CAR Web サービス	235
Cisco SOAP - CDRonDemand Service	235
セキュリティ サービス	236
Cisco CTL Provider	236
Cisco Certificate Authority Proxy Function (CAPF)	236
ディレクトリ サービス	236
Cisco DirSync	236
ロケーションベースのトラッキング サービス	237
Cisco Wireless Controller Synchronization サービス	237
Voice Quality Reporter Services	237
Cisco Extended Functions	238
ネットワーク サービス	238
パフォーマンスおよびモニタリング サービス (Performance and Monitoring Services)	238
バックアップおよび復元サービス	239
System Services	239
プラットフォーム サービス	240
セキュリティ サービス	243
データベース サービス	244

SOAP サービス	244
CM サービス (CM Services)	245
IM and Presence Service サービス	246
CDR サービス	248
インストール	249
サービスのセットアップ	250
コントロールセンター	250
サービスのセットアップ	251
サービス アクティベーション	251
Cisco Unified Communications Manager のクラスタ サービス アクティベーションに関する 推奨事項	252
IM and Presence Service のクラスタ サービス アクティベーションに関する推奨事項	256
機能サービスのアクティブ化	260
コントロールセンターまたは CLI でのサービスの開始、停止、再起動	262
コントロールセンターでのサービスの開始、停止、再起動	262
コマンドライン インターフェイスを使用したサービスの開始、停止、再起動	263
<hr/>	
第 17 章	Trace 265
	Trace 265
	トレース設定 266
	トレース設定 267
	トレース収集 267
	着信側トレース 268
	トレース設定のセットアップ 268
	トレースの設定 269
	トレース パラメータの設定 269
	トレース設定でのサービス グループ 272
	デバッグ トレース レベルの設定 278
	トレース フィールドの説明 279
	Database Layer Monitor のトレース フィールド 279
	Cisco RIS Data Collector のトレースのフィールド 280

Cisco CallManager SDI のトレース フィールド	281
Cisco CallManager SDL のトレース フィールド	283
Cisco CTIManager SDL のトレース フィールド	285
Cisco Extended Functions のトレース フィールド	287
Cisco エクステンション モビリティのトレース フィールド	288
Cisco IP Manager Assistant のトレース フィールド	288
Cisco IP Voice Media Streaming App のトレース フィールド	289
Cisco TFTP のトレース フィールド	290
Cisco WebDialer Web サービスのトレース フィールド	290
IM and Presence SIP Proxy サービスのトレース フィルタの設定	291
IM and Presence トレースフィールドの説明	293
Cisco Access Log のトレースのフィールド	293
Cisco Authentication のトレースのフィールド	293
Cisco Calendar のトレースのフィールド	293
Cisco CTI ゲートウェイのトレースのフィールド	294
Cisco Database Layer Monitor のトレースのフィールド	294
Cisco Enum のトレース フィールド	294
Cisco Method/Event のトレース フィールド	295
Cisco Number Expansion のトレース フィールド	295
Cisco Parser のトレース フィールド	295
Cisco Privacy のトレースのフィールド	295
Cisco Proxy のトレース フィールド	295
Cisco RIS Data Collector のトレースのフィールド	296
Cisco Registry のトレースのフィールド	296
Cisco Routing のトレースのフィールド	297
Cisco Server のトレースのフィールド	297
Cisco SIP Message と State Machine のトレースのフィールド	297
Cisco SIP TCP のトレース フィールド	297
Cisco SIP TLS のトレースのフィールド	298
Cisco Web Service のトレースのフィールド	298
Trace Output Settings	298

トレース設定のトラブルシューティング	299
トラブルシューティング トレース設定ウィンドウ	299
トラブルシューティング トレース設定	300

第 18 章**使用状況レコードの表示 303**

使用状況レコードの概要	303
依存関係レコード	303
ルート プラン レポート	303
使用状況レポートのタスク	304
ルート プラン レポートのタスク フロー	305
ルート プラン レコードの表示	305
ルート プラン レコードの保存	306
未割り当ての電話番号の削除	306
未割り当ての電話番号の更新	307
依存関係レコード タスク フロー	308
依存関係レコードの設定	308
依存関係レコードの表示	309

第 19 章**エンタープライズ パラメータの管理 311**

エンタープライズ パラメータの概要	311
エンタープライズ パラメータ情報の表示	311
エンタープライズ パラメータの更新	312
デバイスへの設定の適用	312
デフォルト エンタープライズ パラメータの復元	313

第 20 章**サーバの管理 315**

サーバの管理の概要	315
サーバの削除	315
クラスタからの Unified Communications Manager ノードの削除	317
クラスタからの IM and Presence ノードの削除	317
削除したサーバをクラスタに戻す	318

インストール前のクラスタへのノードの追加	319
プレゼンス サーバのステータスの表示	320
ポートの設定	321
ポート設定	322
ホスト名の設定	323
Kerneldump ユーティリティ	324
Kerneldump ユーティリティの有効化	325
コア ダンプの電子メール アラートの有効化	326

 第 V 部 :

レポートの管理 329

 第 21 章

Cisco Serviceability Reporter 331

サービスアビリティ レポートのアーカイブ	331
Cisco Serviceability Reporter 設定タスク フロー	332
Cisco Serviceability Reporter のアクティブ化	332
Cisco Serviceability Reporter の設定	333
日次レポート アーカイブの表示	334
日次レポートの概要	334
デバイス統計レポート	334
サーバ統計レポート	337
サービス統計レポート	340
コール アクティビティ レポート	343
アラート要約レポート	347
パフォーマンス保護レポート	349

 第 22 章

Cisco Unified Reporting 351

統合されたデータのレポート	351
レポートの生成に使用するデータ ソース	351
サポートされている出力形式	352
システム要件	352
必要なアクセス権限	353

UI のコンポーネント	353
管理インターフェイスからのログイン	354
サポートされているレポート	355
Unified Communications Manager レポート	355
IM and Presence Service レポート	358
レポートの説明の表示	359
新規レポートの作成	360
保存済みレポートの表示	361
新しいレポートのダウンロード	362
保存済みレポートのダウンロード	362
レポートのアップロード	363

第 23 章

Cisco IP Phone電話の通話診断と品質レポートを設置する 365

診断およびレポートの概要	365
コール診断の概要	365
品質レポートツールの概要	366
詳細なコール レポートおよび課金情報	366
前提条件	366
コール診断の要件	366
品質レポートツールの要件	367
Diagnostics and Reporting の設定タスク フロー	368
コール診断の設定	369
品質レポート ツールの設定	369
QRT ソフトキーを含むソフトキー テンプレートの設定	370
共通デバイス設定と QRT ソフトキー テンプレートの関連付け	372
電話機への QRT ソフトキー テンプレートの追加	373
Cisco Unified Serviceability での QRT の設定	374
品質レポートツールのサービスパラメータの設定	377

第 VI 部 :

セキュリティの管理 381

第 24 章

SAML シングル サインオンの管理 383

- SAML シングル サインオンの概要 383
- iOS 上での Cisco Jabber の証明書ベースの SSO 認証のオプション制御 383
- SAML シングル サインオンの前提条件 384
- SAML シングル サインオンの管理 385
 - SAML シングル サインオンの有効化 385
 - iOS Cisco Jabber の SSO ログインの動作設定 386
 - アップグレード後の WebDialer 上での SAML シングル サインオンの有効化 387
 - Cisco WebDialer サービスの非アクティブ化 387
 - SAML シングル サインオンの無効化 388
 - Cisco WebDialer サービスのアクティブ化 388
 - リカバリ URL へのアクセス 389
 - ドメインまたはホスト名変更後のサーバメタデータの更新 389
 - サーバ削除後にサーバのメタデータを更新する 390
 - サーバメタデータの手動プロビジョニング 391

第 25 章

証明書の管理 393

- 証明書の概要 393
 - サードパーティの署名付き証明書または証明書チェーン 394
 - サードパーティ認証局証明書 395
 - 証明書署名要求のキー用途拡張 396
- 証明書の表示 397
- 証明書のダウンロード 398
- 中間証明書のインストール 398
- 信頼証明書の削除 399
- 証明書の再作成 400
 - 証明書の名前と説明 401
 - OAuth 更新ログイン用のキーの再生成 402
- 証明書または証明書チェーンのアップロード 403
- サードパーティ証明書の認証局の管理 404

証明書署名要求の生成	405
証明書署名要求のダウンロード	406
信頼ストアへの認証局署名済み CAPF ルート証明書の追加	406
サービスの再起動	407
オンライン証明書ステータス プロトコル (OCSP) による証明書失効 (CRL)	407
証明書モニタリング タスク フロー	409
証明書モニタ通知の設定	409
OCSP による証明書失効の設定	410
証明書エラーのトラブルシュート	411

第 26 章

一括証明書の管理	413
一括証明書の管理	413
証明書のエクスポート	413
証明書のインポート	414

第 27 章

IPSec ポリシーの管理	417
IPsec ポリシーの概要	417
IPsec ポリシーの設定	418
IPsec 証明書の確認	419
IPSec ポリシーの管理	419

第 28 章

クレデンシャル ポリシーの管理	421
クレデンシャル ポリシーと認証	421
クレデンシャル ポリシーの JTAPI および TAPI のサポート	422
クレデンシャル ポリシーの設定	422
クレデンシャル ポリシー デフォルトの設定	423
認証アクティビティのモニタ	423
クレデンシャル キャッシングの設定	425
セッションの終了の管理	425

第 VII 部 :

IP アドレス、ホスト名、およびドメイン名の変更	427
---------------------------------	------------

第 29 章	変更前タスクとシステムヘルスチェック	429
	変更前のタスク	429
	IP アドレス、ホスト名、およびその他のネットワーク識別子の変更	429
	IM and Presence Service ノード名およびデフォルトのドメイン名の変更	430
	ホスト名の設定	430
	手順のワークフロー	432
	Cisco Unified Communications Manager ワークフロー	432
	IM and Presence Service のワークフロー	433
	Cisco Unified Communications Manager ノードの変更前タスク	434
	IM and Presence サービス ノードの変更前セットアップタスク	436

第 30 章	IP アドレスおよびホスト名の変更	441
	IP アドレスとホスト名の変更のタスク リスト	441
	OS Admin GUI による IP アドレスまたはホスト名の変更	442
	Unified CM の管理 GUI による IP アドレスまたはホスト名の変更	443
	CLI による IP アドレスまたはホスト名の変更	444
	Set Network Hostname の CLI 出力例	446
	IP アドレスのみの変更	447
	ネットワーク IP アドレスの設定の出力例	448
	CLI による IP アドレスまたはホスト名の変更	448

第 31 章	ドメイン名およびノード名の変更	451
	ドメイン名の変更	451
	IM and Presence サービスのデフォルトドメイン名の変更作業	452
	DNS レコードの更新	453
	FQDN 値でのノード名の更新	455
	DNS ドメインの更新	456
	クラスタノードに関する考慮事項	457
	セキュリティ証明書の再生成	458
	ノード名の変更	459

IM and Presence Service ノード名の変更作業リスト	460
ノード名の更新	461
CLI を使用したノード名の変更の確認	462
Cisco Unified CM IM and Presence Administration を使用したノード名の変更の検証	462
Cisco Unified Communications Manager のドメイン名の更新	463

第 32 章

変更後のタスクと検証 465

Cisco Unified Communications Manager ノードの変更後タスク	465
Cisco Unified Communications Manager ノードのセキュリティを有効にしたクラスタ タスク	469
初期信頼リストおよび証明書の再生成	469
シングルサーバクラスタ電話機の証明書と ITL の再生成	469
マルチサーバクラスタ電話機の証明書と ITL の再生成	470
IM and Presence Service ノードの変更後タスク	470

第 33 章

アドレス変更に関する問題のトラブルシューティング 475

クラスタ認証のトラブルシューティング	475
データベース レプリケーションのトラブルシューティング	476
データベースのレプリケーションの確認	476
データベース レプリケーションの CLI 出力例	477
データベース レプリケーションの修復	478
データベース レプリケーションのリセット	480
ネットワークをトラブルシューティング	481
ネットワーク タイムプロトコル (NTP) のトラブルシューティング	482
サブスクリバ ノードにおける NTP のトラブルシューティング	482
パブリッシャ ノードにおける NTP のトラブルシューティング	482

第 VIII 部 :

ディザスタリカバリ 485

第 34 章

システムのバックアップ 487

バックアップの概要	487
-----------	-----

バックアップの前提条件	489
バックアップタスクフロー	490
バックアップデバイスの設定	491
バックアップファイルのサイズの予測	492
スケジュールバックアップの設定	493
手動バックアップの開始	494
現在のバックアップステータスの表示	495
バックアップ履歴の表示	496
バックアップの連携動作と制約事項	496
バックアップの制約事項	497
リモートバックアップ用 SFTP サーバ	497

 第 35 章

システムの復元 501

復元の概要	501
マスターエージェント	501
ローカルエージェント	502
復元の前提条件	502
復元タスクフロー	503
最初のノードのみの復元	504
後続クラスタノードの復元	506
パブリッシャの再構築後の 1 回のステップでのクラスタの復元	508
クラスタ全体の復元	510
前回正常起動時の設定へのノードまたはクラスタの復元	511
ノードの再起動	512
復元ジョブステータスのチェック	513
復元履歴の表示	513
データ認証	514
トレースファイル	514
コマンドラインインターフェイス	514
アラームおよびメッセージ	516
アラームおよびメッセージ	516

ライセンス予約	519
ライセンス予約	519
ライセンス情報	520
ライセンス情報	520
復元の連携動作と制約事項	522
復元の連携動作と制約事項	522
トラブルシューティング	523
より小さい仮想マシンへの DRS 復元の失敗	523

 第 IX 部 :

トラブルシューティング 525

第 36 章

トラブルシューティングの概要 527

Cisco Unified Serviceability	527
Cisco Unified Communications Operating System Administration	528
一般的な問題解決モデル	528
ネットワーク障害への事前準備	529
詳細情報の入手先	530

第 37 章

トラブルシューティング ツール 531

Cisco Unified サービスアビリティ	トラブルシューティング ツール	531
コマンドライン インターフェイス		533
Kerneldump ユーティリティ		533
Kerneldump ユーティリティの有効化		534
コア ダンプの電子メールアラートの有効化		535
ネットワーク管理		536
システム ログ管理		536
Cisco Discovery Protocol のサポート		537
簡易ネットワーク管理プロトコル (SNMP) のサポート		537
スニファ	トレース	538
デバッグ		538
Cisco Secure Telnet		539

パケット キャプチャ	539
パケット キャプチャの概要	539
パケット キャプチャの設定チェックリスト	540
Standard Packet Sniffer Users アクセス コントロールグループへのエンド ユーザの追加	541
パケット キャプチャのサービス パラメータの設定	541
[電話の設定 (Phone Configuration)] ウィンドウでのパケット キャプチャの設定	542
[ゲートウェイの設定 (Gateway Configuration)] ウィンドウおよび[トランクの設定 (Trunk Configuration)] ウィンドウでのパケット キャプチャの設定	543
パケット キャプチャの設定値	545
キャプチャしたパケットの分析	547
一般的なトラブルシューティングのタスク、ツール、およびコマンド	547
トラブルシューティングのヒント	550
システム履歴ログ	552
システム履歴ログの概要	552
システム履歴ログのフィールド	553
システム履歴ログへのアクセス	554
監査ロギング	555
Cisco Unified Communications Manager サービスが稼働しているかどうかの確認	560

第 38 章

TAC とのケースのオープン	563
必要な情報	564
必要な予備的信息	564
ネットワーク レイアウト	564
問題の説明	565
一般情報	565
TAC Case Open ツールのオンライン サービス	566
Serviceability Connector	566
Serviceability Connector の概要	566
Serviceability サービスを使用する利点	567
Serviceability Connector の TAC サポート	567
Cisco Live!	567

リモート アクセス	568
Cisco Secure Telnet	568
ファイアウォールによる保護	569
Cisco Secure Telnet の設計	569
Cisco Secure Telnet の構造	569
リモート アカウントの設定	570



CHAPTER 1

新機能と更新情報

- [新機能と更新情報, on page 1](#)

新機能と更新情報

次の表は、この最新リリースまでのガイドでの機能の主な変更点の概要を示したものです。ただし、今リリースまでのガイドにおける変更点や新機能の一部は表に記載されていません。

Table 1: Unified Communications Manager と IM and Presence サービスの新機能と変更された動作

機能または変更	説明	参照先	日付
リリース 14 のマニュアルの初回リリース	—	—	2021 年 3 月 31 日
リリース 14SU1 のマニュアルの初回リリース	—	—	2021 年 10 月 27 日
TFTP サーバーからの大きなファイルのダウンロードのサポート	Unified Communications Manager は、TFTP およびプロキシ TFTP での HTTP 範囲要求 (RFC7233) をサポートします (ダウンロードファイルが 100MB 以上の場合)。	ファームウェアのインストールの潜在的な問題, on page 95	2021 年 10 月 27 日

機能または変更	説明	参照先	日付
パーマネントライセンスの予約	この機能を使用すると、製品インスタンスに対して、スマートアカウントおよびバーチャルアカウントから権限のある永久ライセンスタグを予約できます。	ライセンス予約, on page 519	2021年10月27日
リリース 14SU2 のマニュアルの初回リリース	—	—	2022年6月16日
ライセンスのディザスタリカバリシステム	ライセンス予約の復元された状態を更新しました	ライセンス情報, on page 520	2022年6月16日



第 Ⅰ 部

管理の概要

- [管理の概要](#) (5 ページ)
- [はじめに](#) (13 ページ)



第 2 章

管理の概要

- [Cisco Unified CM Administration の概要](#) (5 ページ)
- [オペレーティング システムの管理の概要](#) (6 ページ)
- [Cisco Unified Serviceability の概要](#) (9 ページ)
- [Cisco Unified Reporting の概要](#) (10 ページ)
- [ディザスタ リカバリ システムの概要](#) (11 ページ)
- [一括管理ツールの概要](#) (12 ページ)

Cisco Unified CM Administration の概要

Cisco Unified CM の管理は、Cisco Unified Communications Manager の主要な管理および設定インターフェイスとなる、Web ベースのアプリケーションです。Cisco Unified CM の管理を使用して、一般的なシステム コンポーネント、機能、サーバ設定、コールルーティングルール、電話機、エンドユーザ、メディア リソースなど、システムの幅広い項目を設定できます。

設定メニュー

Cisco Unified CM の管理の設定ウィンドウは、以下のメニューで編成されています。

- [システム (System)] : このメニューに分類されている設定ウィンドウを使用して、一般的なシステム設定 (サーバ情報、NTP 設定、日時グループ、リージョン、DHCP、LDAP 統合、エンタープライズ パラメータなど) を構成します。
- [コールルーティング (Call Routing)] : このタブに分類されている設定ウィンドウを使用して、Cisco Unified Communications Manager によるコールのルーティング方法に関連する項目 (ルート パターン、ルート グループ、ハントパイロット、ダイヤルルール、パーティション、コール サーチ スペース、電話番号、変換パターンなど) を設定します。
- [メディア リソース (Media Resources)] : このタブに分類されている設定ウィンドウを使用して、メディア リソース グループ、会議ブリッジ、アナウンサー、トランスコーダなどの項目を設定します。
- [拡張機能 (Advanced Features)] : このタブに分類されている設定ウィンドウを使用して、ボイスメールパイロット、メッセージ受信、コール制御エージェント プロファイルなどの機能を設定します。

- [デバイス (Device)] : このタブに分類されている設定ウィンドウを使用して、電話機などのデバイス、IP Phone サービス、トランク、ゲートウェイ、ソフトキーテンプレート、SIP プロファイルを設定します。
- [アプリケーション (Application)] : このタブに分類されている設定ウィンドウを使用して、Cisco Unified JTAPI、Cisco Unified TAPI、Cisco Unified Real-Time Monitoring Tool などのプラグインをダウンロードおよびインストールします。
- [ユーザ管理 (User Management)] : [ユーザ管理 (User Management)] タブに分類されている設定ウィンドウを使用して、システムのエンドユーザおよびアプリケーションユーザを設定します。
- [一括管理 (Bulk Administration)] : 一括管理ツールを使用して、多数のエンドユーザやデバイスを同時にインポートおよび設定します。
- [ヘルプ (Help)] : このメニューをクリックすることで、オンラインヘルプシステムにアクセスできます。オンラインヘルプシステムには、システム上の各種設定ウィンドウの設定を構成する際に役立つドキュメントが含まれています。

オペレーティングシステムの管理の概要

[Cisco Unified Communications オペレーティングシステムの管理 (Cisco Unified Communications Operating System Administration)] を使用して、オペレーティングシステムの設定と管理、および以下の管理タスクを実行します。

- ソフトウェアとハードウェアのステータスを確認する
- IP アドレスを確認および更新する
- 他のネットワーク デバイスに ping を送信する
- NTP サーバを管理する
- システム ソフトウェアおよびオプションをアップグレードする
- ノードのセキュリティを管理する (IPSec や証明書を含む)
- リモート サポート アカウントを管理する
- システムを再起動する

オペレーティングシステムのステータス

以下のものを含め、各種のオペレーティングシステム コンポーネントのステータスを確認できます。

- クラスタおよびノード
- ハードウェア
- ネットワーク
- システム
- インストールされているソフトウェアとオプション

オペレーティング システムの設定

オペレーティング システムの次の設定を表示し、更新できます。

- [IP] : アプリケーションのインストール時に入力した IP アドレスおよび DHCP クライアントの設定を更新します。
- [NTP サーバの設定 (NTP Server Settings)] : 外部 NTP サーバの IP アドレスの設定、および NTP サーバの追加を行います。
- [SMTP 設定 (SMTP settings)] : オペレーティング システムが E メール通知の送信に使用する Simple Mail Transfer Protocol (SMTP) ホストを設定します。

オペレーティング システムのセキュリティ設定

セキュリティ証明書および IPsec の設定を管理できます。[セキュリティ (Security)] メニューでは、次のセキュリティ オプションを選択できます。

- [証明書の管理 (Certificate Management)] : 証明書および証明書署名要求 (CSR) を管理します。証明書の表示、アップロード、ダウンロード、削除、および再作成を行うことができます。[証明書の管理 (Certificate Management)] を使用して、ノード上の証明書の有効期限をモニタすることもできます。
- [IPsec の管理 (IPsec Management)] : 既存の IPsec ポリシーの表示や更新、新規の IPsec ポリシーとアソシエーション設定を行います。

ソフトウェアのアップグレード

オペレーティング システムで実行中のソフトウェア バージョンをアップグレードしたり、特定のソフトウェア オプション (Cisco Unified Communications オペレーティング システム ロケール インストーラ、ダイヤルプラン、TFTP サーバファイルなど) をインストールできます。

[インストール/アップグレード (Install/Upgrade)] メニュー オプションで、ローカルディスクまたはリモート サーバからシステム ソフトウェアをアップグレードできます。アップグレードしたソフトウェアは非アクティブなパーティションにインストールされ、その後でシステムの再起動とパーティションの切り替えができます。これにより、システムで新しいソフトウェア バージョンが実行されます。詳細については、『*Upgrade Guide for the Cisco Unified Communications Manager*』 (<http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-guides-list.html>) を参照してください。



- (注) Cisco Unified Communications オペレーティング システムのインターフェイスと CLI に含まれるソフトウェアアップグレード機能を使用して、すべてのソフトウェアのインストールとアップグレードを実行する必要があります。このシステムでアップロードおよび処理できるソフトウェアは、シスコによって承認されたものだけです。サードパーティー製または Windows ベースのソフトウェア アプリケーションはインストールまたは使用できません。

サービス

このアプリケーションでは、次のオペレーティングシステムユーティリティを使用できます。

- ping : 他のネットワーク デバイスとの接続を確認します。
- リモートサポート : シスコのサポート担当者がシステムへのアクセスに使用できるアカウントを設定します。このアカウントは、指定した日数が経過すると自動的に失効します。

CLI

CLI には、オペレーティング システムからアクセスすることも、サーバへのセキュア シェル 接続を使用してアクセスすることもできます。詳細については、『*Command Line Interface Reference Guide for Cisco Unified Communications Solutions*』（<http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html>）を参照してください。

認証済み Network Time Protocol のサポート

Cisco Unified Communications Manager リリース 12.0(1) では、Unified Communications Manager の認証済み Network Time Protocol (NTP) 機能がサポートされています。このサポートは、Unified Communications Manager へのセキュアな NTP サーバ接続を確立するために追加されています。以前のリリースでは、NTP サーバに対する Unified Communications Manager の接続はセキュアではありませんでした。

この機能は、対称キーベースの認証に基づいており、NTPv3 および NTPv4 サーバによってサポートされています。Unified Communications Manager は、SHA1 ベースの暗号化のみをサポートしています。SHA1 ベースの対称キーのサポートは、NTP バージョン 4.2.6 以降で利用できます。

- 対称キー
- 認証なし

NTP サーバの認証ステータスは、**Cisco Unified OS の管理アプリケーション**の管理 CLI または [NTPサーバの一覧 (NTP Server List)] ページで確認できます。

自動キー認証済み Network Time Protocol のサポート

Cisco Unified Communications Manager は、自動キー機能（公開キー インフラストラクチャベースの認証）による Network Time Protocol (NTP) 認証もサポートしています。この機能は、パブリッシャ ノードでのみ適用できます。

RedHat は自動キーよりも対称キー認証を推奨しています。詳細については、<https://access.redhat.com/support/cases/#/case/01871532>を参照してください。

この機能は、コモン クライテリア認定のために PKI ベースの認証が必須であるため追加されました。

Cisco Unified Communication Manager でコモンクライテリア モードを有効にしている場合にのみ、NTP サーバで IFF ID スキームによる PKI ベースの認証を設定できます。

Cisco Unified Communications Manager で、対称キーまたは PKI ベースの NTP 認証を有効にできます。

PKI 対応サーバで対称キーを有効にしようとすると、次の警告メッセージが表示されます。



警告 Autokeyを使用したNTP認証が現在有効になっており、対称キーを有効にする前に無効にする必要があります。(NTP authentication using Autokey is currently enabled and must be disabled before the symmetric key is enabled.) コマンド「`utils ntp auth auto-key disable`」を使用してNTP認証を無効にしてから、このコマンドを再実行してください。(Use the command 'utils ntp auth auto-key disable' to disable NTP authentication, then retry this command.)

対称キー対応サーバで Autokey を有効にしようとすると、次の警告メッセージが表示されます。



警告 対称キーを使用するNTP認証が現在有効になっており、Autokeyを有効にする前に無効にする必要があります。(NTP authentication using symmetric key is currently enabled and must be disabled before Autokey is enabled.) コマンド「`utils ntp auth symmetric-key disable`」を使用してNTP認証を無効にしてから、このコマンドを再実行してください。(Use the command 'utils ntp auth symmetric-key disable' to disable NTP authentication, then retry this command.)



(注) NTP サーバには ntp バージョン 4 と rpm バージョン ntp-4.2.6p5-1.el6.x86_64.rpm 以上が必要です。

NTP サーバの認証ステータスは、Cisco Unified OS の管理アプリケーションの管理 CLI または [NTPサーバの一覧(NTP Server List)] ページで確認できます。

Cisco Unified Serviceability の概要

Cisco Unified Serviceability は、管理者がシステムを管理する際の、サービス、アラーム、支援ツールのホストを提供する、Web ベースのトラブルシューティング ツールです。Cisco Unified Serviceability が提供する機能を利用して、管理者は以下の作業を行うことができます。

- サービスの開始と停止：管理者はシステムを管理する上で役立つさまざまなサービスを設定できます。たとえば、Cisco CallManager Serviceability RTMT サービスを開始することにより、管理者は Real-Time Monitoring Tool を使ってシステムの正常性をモニタできます。
- SNMP：アプリケーション層プロトコルである SNMP を使用すると、ノードやルータなどのネットワーク デバイス間の管理情報を簡単に交換できます。TCP/IP プロトコルスイートの一部である SNMP を使用すると、管理者はリモートでネットワークのパフォーマンス

を管理し、ネットワークの問題を検出および解決し、ネットワークの拡張計画を立てることができます。

- アラーム：アラームは、システムの実行時のステータスと状態に関する情報を提供するため、システムに関する問題をトラブルシューティングできます。
- トレース：トレースツールは、音声アプリケーションの問題をトラブルシューティングするのに役立ちます。
- Cisco Serviceability Reporter：Cisco Serviceability Reporter は、Cisco Unified Serviceability 内で日次レポートを生成します。
- SNMP：アプリケーション層プロトコルである SNMP を使用すると、ノードやルータなどのネットワーク デバイス間の管理情報を簡単に交換できます。TCP/IP プロトコルスイートの一部である SNMP を使用すると、管理者はリモートでネットワークのパフォーマンスを管理し、ネットワークの問題を検出および解決し、ネットワークの拡張計画を立てることができます。
- CallHome：Cisco Unified Communications Manager の Call Home 機能を設定し、Cisco Unified Communications Manager が通信し、診断アラート、インベントリおよびその他のメッセージを Smart Call Home バックエンド サーバに送信できるようにします。

その他の管理インターフェイス

Cisco Unified Serviceability を使用して、サービスを開始し以下の他の管理インターフェイスを使用できます。

- Real-Time Monitoring Tool：Real-Time Monitoring Tool は、システムの正常性をモニタするために利用できる Web ベースのインターフェイスです。RTMT を使用して、アラームやカウンタを確認したり、システムの正常性に関する詳細情報が記載されたレポートを表示したりできます。
- Dialed Number Analyzer：Dialed Number Analyzer は、管理者がダイヤルプランの問題をトラブルシューティングする際に役立つ、Web ベースのインターフェイスです。
- Cisco Unified CDR Analysis and Reporting：CDR Analysis and Reporting は、システムで行われたコールの詳細を記録したレコードを収集します。

Cisco Unified Serviceability の使用方法の詳細については、『*Cisco Unified Serviceability Administration Guide*』（<http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html>）を参照してください。

Cisco Unified Reporting の概要

Cisco Unified Reporting Web アプリケーションは、クラスタ データをトラブルシューティングまたは検査するための統合レポートを生成します。このアプリケーションには、Unified

Communications Manager および Unified Communications Manager IM and Presence Service のコンソールでアクセスできます。

このツールは、クラスタデータのスナップショットを簡単に作成する方法を提供します。このツールは、既存のソースからのデータの収集、データの比較、および異常の報告を行います。Cisco Unified Reporting で生成されるレポートは、1 台以上のサーバの 1 つ以上のソースからのデータを 1 つの出力ビューに統合します。システムを管理する際には、たとえば以下のレポートを表示して利用できます。

- [Unified CM クラスタ概要 (Unified CM Cluster Overview)] : Cisco Unified Communications Manager and IM and Presence Service のバージョン、サーバのホスト名、ハードウェアの詳細といったクラスタのスナップショットを取得するときに、このレポートを参照します。
- [電話機機能リスト (Phone Feature List)] : 機能を設定する際は、このレポートを表示します。このレポートは、どの電話機がどの Unified Communications Manager 機能をサポートしているかを一覧します。
- [回線未使用の Unified CM 電話 (Unified CM Phones Without Lines)] : 電話回線を使用していない、クラスタ内の電話機を確認するには、このレポートを表示します。

Cisco Unified Reporting が提供するレポートをすべて網羅したリスト、およびこのアプリケーションの使用方法については、『Cisco Unified Reporting Administration Guide』

(<http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html>) を参照してください。

ディザスタリカバリシステムの概要

ディザスタリカバリシステム (DRS) は、[Cisco Unified Communications Manager 管理 (Cisco Unified Communications Manager Administration)] から呼び出すことができるシステムで、完全なデータバックアップおよび復元の機能を提供します。ディザスタリカバリシステムでは、定期的にスケジュールされた自動データバックアップまたはユーザ起動のデータバックアップを実行できます。

DRS は、プラットフォームのバックアップ/復元の一環として、独自の設定 (バックアップデバイス設定およびスケジュール設定) を復元します。DRS は drfDevice.xml ファイルと drfSchedule.xml ファイルをバックアップおよび復元します。これらのファイルとともにサーバを復元するときは、DRS バックアップデバイスおよびスケジュールを再設定する必要があります。

ディザスタリカバリシステムには、次の機能があります。

- バックアップおよび復元タスクを実行するためのユーザインターフェイス。
- バックアップおよび復元機能を実行するための分散システムアーキテクチャ。
- バックアップのスケジューリング。
- 物理的なテープドライブまたはリモート SFTP サーバへのバックアップのアーカイブ。

一括管理ツールの概要

Cisco Unified Communications Manager 内にエンティティを設定するには、Unified CM の管理の [一括管理 (Bulk Administration)] メニューおよびサブメニュー オプションで一括管理ツールを使用します。

Unified Communications Manager の一括管理ツール (BAT) は Web ベースのアプリケーションであり、管理者が Unified Communications Manager データベースに対する一括トランザクションを行うために使用できます。BAT では、多数の同じような電話、ユーザ、またはポートを同時に追加、更新、削除できます。Cisco Unified CM の管理を使用する場合、データベース トランザクションごとに個々の手動操作が必要になりますが、BAT はこのプロセスを自動化し、追加、更新、削除の操作を短時間で実行できるようにします。

以下のタイプのデバイスとレコードを処理する場合は BAT を使用できます。

- Cisco IP Phone、ゲートウェイ、電話機、Computer Telephony Interface (CTI) ポート、H.323 クライアントの追加、更新、削除
- ユーザ、ユーザ デバイス プロファイル、Cisco Unified Communications Manager Assistant マネージャおよびアシスタントの追加、更新、削除
- 強制承認コードとクライアント マター コードの追加、削除
- コール ピックアップ グループの追加、削除
- リージョン マトリクスの実装、実装解除
- アクセス リストの挿入、削除、エクスポート
- リモート宛先およびリモート宛先 プロファイルの挿入、削除、エクスポート
- インフラストラクチャ デバイスの追加

一括管理ツールの使用方法の詳細については、『*Bulk Administration Guide for Cisco Unified Communications Manager*』を参照してください。



第 3 章

はじめに

- [管理インターフェイスへのログイン \(13 ページ\)](#)
- [管理者またはセキュリティ パスワードのリセット \(13 ページ\)](#)
- [システムのシャットダウンまたは再起動 \(15 ページ\)](#)

管理インターフェイスへのログイン

システム内の管理インターフェイスのいずれかにサインインする場合に、次の手順を使用します。

手順

- ステップ 1** ご使用の Web ブラウザで、Unified Communications Manager インターフェイスを開きます。
 - ステップ 2** [ナビゲーション (Navigation)] ドロップダウン リストから管理インターフェイスを選択します。
 - ステップ 3** [移動 (Go)] をクリックします。
 - ステップ 4** ユーザ名とパスワードを入力します。
 - ステップ 5** [ログイン (Login)] をクリックします。
-

管理者またはセキュリティ パスワードのリセット

管理者パスワードを消失し、システムにアクセスできない場合は、次の手順を使用してパスワードをリセットします。



- (注) IM and Presence ノードでのパスワードの変更については、管理者パスワードをリセットする前に、すべての IM およびプレゼンスノードで Cisco Presence Engine サービスを停止します。パスワードをリセットした後、すべてのノードで Cisco Presence Engine サービスを再起動します。PE が停止したときにプレゼンスの問題が発生する可能性があるため、メンテナンス時にこのタスクを実行してください。

始める前に

- この手順を実行するノードに物理的にアクセスできる必要があります。
- どの時点でも、CD または DVD メディアを挿入するように求められたら、VMWare サーバ用の vSphere クライアントを用いて ISO ファイルをマウントする必要があります。指示については、「『Adding DVD or CD Drives to a Virtual Machine』」 https://www.vmware.com/support/ws5/doc/ws_disk_add_cd_dvd.html を参照してください。
- セキュリティパスワードは、クラスタ内のすべてのノードで一致している必要があります。セキュリティパスワードは、すべてのマシン上で変更してください。変更していない場合、クラスタ ノードが通信不能になります。

手順

ステップ 1 次のユーザ名とパスワードを使用して、パブリッシャ ノードで CLI にサインインします。

- a) ユーザ名 : **pwrecovery**
- b) パスワード : **pwreset**

ステップ 2 何かキーを押して続行します。

ステップ 3 ディスク ドライブに有効な CD または DVD が入っている場合、または ISO ファイルをマウントしてある場合は、VMWare クライアントから取り出します。

ステップ 4 何かキーを押して続行します。

ステップ 5 有効な CD または DVD をドライブに挿入するか、ISO ファイルをマウントします。

- (注) このテストでは、データ専用のディスクまたは ISO ファイルを使用する必要があります。

ステップ 6 最後のステップが確認されると、次のいずれかのオプションを入力して続行するように指示されます。

- **a** を入力して、管理者パスワードをリセットする。
- セキュリティパスワードをリセットする場合は、**s** を入力します。

- (注) セキュリティパスワードを変更したら、クラスタ内の各ノードをリセットする必要があります。ノードをリブートしない場合、システムサービスで問題が発生するほか、サブスクライバサーバ上の管理ウィンドウで問題が発生します。

ステップ7 新しいパスワードを入力し、確認のためにもう一度入力します。

管理者のクレデンシャルは、先頭がアルファベットで6文字以上必要です。英数字、ハイフン、およびアンダースコアを使用できます。

ステップ8 新しいパスワードの強度が検証された後、パスワードがリセットされ、任意のキーを押してパスワードリセットユーティリティを終了するように指示されます。

異なる管理者パスワードを設定する場合は、CLI コマンド **set password** を使用します。詳細については、『*Command Line Interface Reference Guide for Cisco Unified Solutions*』

(<http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html>) を参照してください。

システムのシャットダウンまたは再起動

設定を変更した後などにシステムをシャットダウンまたは再起動する必要がある場合、次の手順を使用します。

始める前に

仮想マシンからサーバのシャットダウンおよび再起動が強制されると、ファイルシステムが破損する可能性があります。強制シャットダウンを回避します。代わりに、この手順の実行後または CLI からの **utils system shutdown** の実行後に、サーバが適切にシャットダウンするまで待ちます。



(注) VMware 管理ツール (vCenter または Embedded Host Client) から仮想マシンを強制的にシャットダウンまたは再起動した場合：

- 12.5 (1) SU3 以前から、これはアングレースフルシャットダウン/再起動となり、ファイルシステムが破損する可能性があります。アングレースフルシャットダウンは、`system-history.log` に表示されます。代わりに、`utils system shutdown` CLI コマンドを使用して正常にシャットダウン/再起動することをお勧めします (これは、`system-history.log` にグレースフルシャットダウン/再起動として表示されます)。

手順

ステップ1 [Cisco Unified OS の管理 (Cisco Unified OS Administration)] から、[設定 (Settings)] > [バージョン (Version)] を選択します。

ステップ2 次のいずれかの操作を実行します。

- すべてのプロセスを停止し、システムをシャットダウンするには、[シャットダウン (Shutdown)] をクリックします。
 - すべてのプロセスを停止し、システムを再起動するには、[再起動 (Restart)] をクリックします。
-



第 II 部

ユーザの管理

- ユーザアクセスの管理 (19 ページ)
- エンドユーザの管理 (49 ページ)
- アプリケーションユーザの管理 (63 ページ)



第 4 章

ユーザ アクセスの管理

- ユーザ アクセスの概要 (19 ページ)
- ユーザ アクセスの前提条件 (24 ページ)
- ユーザ アクセスの設定タスク フロー (24 ページ)
- 非アクティブなユーザ アカウントの無効化 (35 ページ)
- リモート アカウントの設定 (36 ページ)
- 標準ロールとアクセス制御グループ (36 ページ)

ユーザ アクセスの概要

次の項目を設定して、Cisco Unified Communications Manager に対するユーザ アクセスを管理します。

- [アクセス制御グループ (Access Control Groups)]
- [ロール (Roles)]
- [ユーザ ランク (User Rank)]

アクセス制御グループの概要

アクセス制御グループは、ユーザのリストと、それらのユーザに割り当てられているロールのリストです。エンド ユーザ、アプリケーション ユーザ、または管理者ユーザをアクセス制御グループに割り当てると、そのユーザは、そのグループに関連付けられているロールのアクセス権限を取得します。類似するアクセス権限を持つユーザを、必要なロールとアクセス許可のみを含むアクセス制御グループに割り当てることによって、システム アクセスを管理できます。

アクセス制御グループには、次の 2 つのタイプがあります。

- 標準アクセス制御グループ：これらは定義済みのデフォルトグループであり、一般的な導入ニーズを満たすロールが割り当てられています。標準グループ内のロール割り当てを編集することはできません。ただし、ユーザの追加または削除、ユーザのランク要件の編集

は可能です。標準アクセス制御グループのリストと、それらに関連付けられているロールについては、「[標準ロールとアクセス制御グループ \(36 ページ\)](#)」を参照してください。

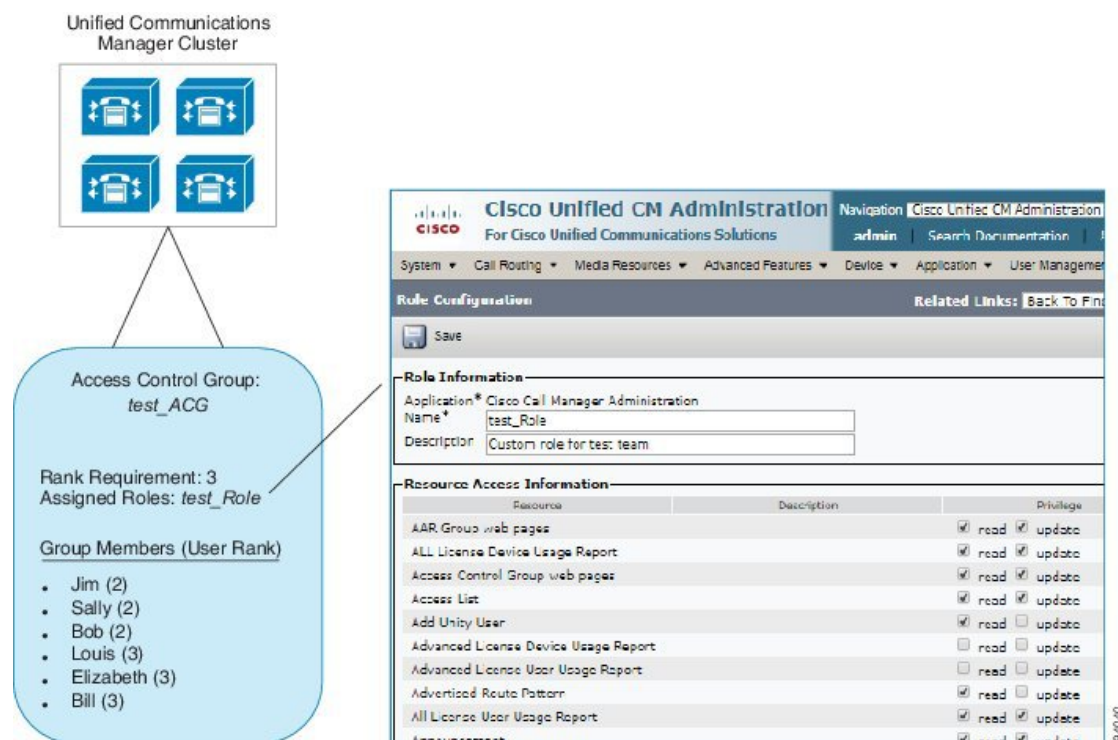
- カスタムアクセス制御グループ：必要条件を満たすロールの権限が標準のグループに含まれていない場合は、独自のアクセス制御グループを作成します。

ユーザランクのフレームワークによって、ユーザの割り当てが可能なアクセス制御グループに対する一連の制御が提供されます。アクセス制御グループにユーザを割り当てるためには、そのグループの最小ランク要件をユーザが満たしている必要があります。たとえば、ユーザランクが4であるエンドユーザは、最小ランク要件が4～10であるアクセス制御グループにのみ割り当てることができます。最小ランクが1のグループには割り当てることができません。

例：アクセス制御グループを使用したロールの権限

次の例は、テストチームのメンバーがアクセス制御グループ **test_ACG** に割り当てられているクラスタを示しています。右側のスクリーンキャプチャには、このアクセス制御グループに関連付けられているロールである **test_Role** のアクセス設定が表示されています。このアクセス制御グループの最小ランク要件は3であることにも注目してください。このグループに参加するためには、すべてのグループメンバーのランクが1～3でなければなりません。

図 1: アクセス制御グループを使用したロールの権限



ロールの概要

ユーザは、そのユーザがメンバーとなっているアクセス制御グループに関連付けられたロールを介して、システムアクセス権限を取得します。各ロールには、Cisco Unified CM Administration または CDR Analysis and Reporting などの特定のリソースまたはアプリケーションに割り当てられた一連の権限が含まれています。Cisco Unified CM Administration などのアプリケーションの場合、ロールには、アプリケーション内の特定の GUI ページを表示または編集できるアクセス許可が含まれている場合があります。リソースまたはアプリケーションに割り当てることができるアクセス許可には、次の 3 つのレベルがあります。

- 読み取り: ユーザがリソースの設定を表示することを許可します。
- [更新 (Update)]: ユーザはリソースの設定を編集できます。
- [アクセスなし (No Access)]: ユーザが読み取りと更新のどちらのアクセス権も持っていない場合、そのユーザは、特定のリソースの設定を表示も編集もできません。

ロールタイプ

ユーザをプロビジョニングする場合は、適用するロールを決定してから、そのロールを含むアクセス制御グループにユーザを割り当てる必要があります。Cisco Unified Communications Manager には、主に 2 つのロールタイプがあります。

- 標準ロール: 一般的な展開のニーズを満たすように設計された、プレインストールされたデフォルトのロールです。標準ロールの権限を編集することはできません。
- カスタム ロール: 必要な権限を持つ標準ロールがない場合に、カスタム ロールを作成します。さらに細かいレベルのアクセス制御が必要な場合は、高度な設定を適用して、管理者がキーのユーザ設定を編集できるように制御することができます。詳細については、該当する項を参照してください。

高度なロール設定

カスタマイズされたロールを作成する際に、[アプリケーション ユーザ (Application User)] と [エンド ユーザ (End User)] 設定ウィンドウで選択されたフィールドに、詳細レベルの制御を追加できます。

[高度なロール設定 (Advanced Role Configuration)] ウィンドウでは、Cisco Unified CM Administration へのアクセスを設定する一方で、次のようなタスクの使用を制限できます。

- ユーザの追加
- パスワードの編集
- ユーザ ランクの編集
- アクセス制御グループの編集

次の表では、この設定で適用できる制御について詳しく説明します。

表 2: 高度なリソース アクセス情報

高度なリソース	アクセス制御
権限情報	<p>アクセス制御グループを追加または編集する機能を次のように制御します。</p> <ul style="list-style-type: none"> • [ビュー (View)] : ユーザは、アクセス制御グループを表示することはできますが、追加、編集、または削除することはできません。 • [更新 (Update)] : ユーザは、アクセス制御グループを追加、編集、または削除できます。 <p>(注) 両方の値が選択されていないと、[権限情報 (Permission Information)] セクションは使用できません。</p> <p>(注) [表示 (View)] を選択した場合、[ユーザは自分のユーザの権限情報を更新できます (User can update Permissions Information for own user)] フィールドが [いいえ (No)] に設定され、無効になります。このフィールドを編集できるようにするには、[権限情報 (Permission Information)] フィールドを [更新 (Update)] に設定する必要があります。</p>
ユーザは自分のユーザの権限情報を更新できる	<p>自分のアクセス権限を編集するユーザの機能を制御します。</p> <ul style="list-style-type: none"> • [はい (Yes)] : ユーザは自分の権限情報を更新できます。 • [いいえ (No)] : ユーザは自分の権限情報を更新できません。ただし、ユーザは、同じまたはより低いランクのユーザの権限情報を表示または変更できます。 <p>(注) [ユーザは自分のユーザの権限情報を更新できます (User can update Permissions Information for own user)] フィールドは [いいえ (No)] に設定され、[権限情報の更新 (Permission Information Update)] チェックボックスがオフの場合は無効になります。</p>

高度なリソース	アクセス制御
ユーザ ランク	<p>ユーザ ランクを変更する機能を制御します。</p> <ul style="list-style-type: none"> • [ビュー (View)] : ユーザは、ユーザ ランクを表示できますが、変更することはできません。 • [更新 (Update)] : ユーザはユーザ ランクを変更できます。 <p>(注) 両方の値が選択されていないと、[ユーザ ランク (User Rank)] セクションは使用できません。</p> <p>(注) [表示 (View)] を選択した場合、[ユーザは自分のユーザ ランクを更新できます (User can update User Rank for own user)] フィールドが [いいえ (No)] に設定され、無効になります。このフィールドを編集できるようにするには、[ユーザ ランク (User Rate)] フィールドを [更新 (Update)] に設定する必要があります。</p>
ユーザは自分のユーザのユーザ ランクを更新できる	<p>自分のユーザ ランクを編集するユーザの機能を制御します。</p> <ul style="list-style-type: none"> • [はい (Yes)] : ユーザは自分のユーザ ランクを更新できます。 • [いいえ (No)] : ユーザは自分のユーザ ランクを更新できません。ただし、同じまたはより低いランクのユーザのランクを表示または変更できます。 <p>(注) [ユーザは自分のユーザのユーザ ランクを更新できます (User can update User Rank for own user)] フィールドは [いいえ (No)] に設定されており、[ユーザー ランク (User Rank)] [更新 (Update)] チェックボックスが選択されていない場合は無効になっています。</p>
新しいユーザの追加	<p>新しいユーザを追加する機能を次のように制御します。</p> <ul style="list-style-type: none"> • [はい (Yes)] : ユーザは、新しいユーザを追加できます。 • [いいえ (No)] : [新規追加 (Add New)] ボタンは使用できません。
[パスワード (Password)]	<p>パスワードを変更する機能を制御します。</p> <ul style="list-style-type: none"> • [はい (Yes)] : ユーザは [アプリケーション ユーザ情報 (Application User Information)] セクションでユーザのパスワードを変更できます。 • [いいえ (No)] : [アプリケーション ユーザ情報 (Application User Information)] セクションで、[パスワード (Password)] と [パスワードの確認 (Confirm Password)] は使用できません。

ユーザランクの概要

ユーザランクのアクセス制御では、管理者がエンドユーザやアプリケーションユーザに提供できるアクセスレベルに対する一連の制御を行います。

エンドユーザやアプリケーションユーザをプロビジョニングする場合、管理者は各ユーザのユーザランクを割り当てる必要があります。管理者は、各アクセス制御グループにもユーザランクを割り当てる必要があります。**Control**グループにアクセスするユーザを追加する場合、管理者は、ユーザのユーザランク要件がグループのランク要件を満たしているグループのみユーザを割り当てることができます。たとえば、あるエンドユーザのユーザランクが3の場合、3～10のユーザランクが設定されているアクセス制御グループに割り当てることができます。ただし、管理者は、そのユーザを1または2のユーザランク要件を持つアクセス制御グループに割り当ててはできません。

管理者は、**[ユーザ順位の設定]**ウィンドウ内に独自のユーザランク階層を作成し、ユーザをプロビジョニングし、アクセス制御グループを使用して、その階層を使用することができます。ユーザランクの階層を設定しない場合や、ユーザをプロビジョニングするとき、または**control**グループにアクセスするときにユーザランクの設定を指定しない場合は、すべてのユーザとアクセス制御グループにはデフォルトのユーザランク1(可能な限り高いランク)が割り当てられます。

ユーザアクセスの前提条件

ユーザに必要なアクセスレベルがわかるように、ユーザのニーズを必ず確認してください。ユーザが必要とするアクセス権限を持つロールを割り当てる必要がありますが、アクセスできないシステムへのアクセスは提供しません。

新しいロールとアクセスコントロールグループを作成する前に、標準のロールとアクセスコントロールグループの一覧を確認して、既存のアクセスコントロールグループに必要なロールとアクセス権限があるかどうかを確認します。詳細については、「[標準ロールとアクセス制御グループ \(36 ページ\)](#)」を参照してください。

ユーザアクセスの設定タスクフロー

以下のタスクを実行して、ユーザアクセスを設定します。

始める前に

デフォルトの役割とアクセス制御グループを使用する場合は、カスタマイズされたロールとアクセス制御グループを作成するためのタスクをスキップできます。ユーザを既存のデフォルトのアクセス制御グループに割り当てることができます。

手順

	コマンドまたはアクション	目的
ステップ 1	ユーザランク階層の設定 (25 ページ)	ユーザランク階層を設定します。このタスクを省略すると、すべてのユーザとアクセスコントロールグループにデフォルトのユーザランク 1 (最高ランク) が割り当てられることに注意してください。
ステップ 2	カスタムロールの作成 (26 ページ)	デフォルトのロールに必要なアクセス権限がない場合は、カスタムロールを作成します。
ステップ 3	管理者の高度なロール設定 (27 ページ)	オプション。カスタムロールの高度な権限を使用すると、管理者によるキーユーザ設定の編集機能を制御できます。
ステップ 4	アクセス制御グループの作成 (28 ページ)	デフォルトグループに必要なロール割り当てがない場合は、カスタムアクセスコントロールグループを作成します。
ステップ 5	アクセス制御グループへのユーザの割り当て (29 ページ)	標準またはカスタムのアクセス制御グループに対してユーザを追加または削除します。
ステップ 6	アクセス制御グループの重複する特権ポリシーの設定 (30 ページ)	オプション。この設定は、ユーザが権限が競合する複数のアクセスコントロールグループに割り当てられている場合に使用されます。

ユーザランク階層の設定

カスタムのユーザランク階層を作成するには、この手順を使用します。



(注) ユーザランク階層を設定しない場合は、すべてのユーザおよびアクセス制御グループにデフォルトで 1 (最高ランク) が割り当てられます。

手順

ステップ 1 Cisco Unified CM Administration から、[ユーザ管理 (User Management)] > [ユーザ設定 (User Settings)] > [ユーザランク (User Rank)] 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** [ユーザランク (User Rank)] ドロップダウン メニューから、1 ~ 10 のランク設定を選択します。最も高いランクは1です。
- ステップ4** [ランク名 (Rank Name)] と [説明 (Description)] 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** ユーザランクをさらに追加するには、この手順を繰り返します。
ユーザおよびアクセス制御グループにユーザランクを割り当てることで、ユーザをどのグループに割り当てることができるかを制御できます。

カスタム ロールの作成

カスタマイズされた権限で新しいロールを作成するには、この手順を使用します。必要な権限を備えた標準のロールがない場合に、この方法を使用できます。ロールを作成する方法は2つあります。

- 新規のロールを白紙の状態から作成して設定するには、[新規追加 (Add New)] ボタンを使用します。
- 必要なアクセス権限に近いアクセス権限が既存のロールにある場合は、[コピー (Copy)] ボタンを使用します。既存のロールの権限を、編集可能な新しいロールにコピーできます。

手順

- ステップ1** Cisco Unified CM Administration で、[ユーザ管理 (User Management)] > [ユーザ設定 (User Settings)] > [権限 (Role)] をクリックします。
- ステップ2** 次のいずれかを実行します。
- 新しいロールを作成するには、[新規追加 (Add New)] をクリックします。このロールを関連付ける [アプリケーション (Application)] を選択し、[次へ (Next)] をクリックします。
 - 既存のロールから設定をコピーするには、[検索 (Find)] をクリックして、既存のロールを開きます。[コピー (Copy)] をクリックし、新しいロールの名前を入力します。[OK] をクリックします。
- ステップ3** このロールの [名前 (Name)] と [説明 (Description)] を入力します。
- ステップ4** リソースごとに、該当するチェックボックスをオンにします。
- ユーザがリソースの設定を表示できるようにする場合には、[読み取り (Read)] チェックボックスをオンにします。
 - ユーザがリソースの設定を編集できるようにする場合は、[更新 (Update)] チェックボックスをオンにします。
 - リソースに対するアクセスを提供しない場合は、両方のチェックボックスをオフにします。

ステップ 5 この権限のページに表示されるすべてのリソースに特権を付与する場合は、[すべてにアクセス権を付与 (Grant access to all)] ボタンをクリックし、すべてのリソースから特権を削除する場合は、[すべてにアクセスを許可しない (Deny access to all)] をクリックします。

(注) リソースのリストが複数のページにわたって表示される場合、このボタンは、現在のページに表示されるリソースに限り適用されます。他のページのリストにあるリソースのアクセス権を変更するには、それらのページを表示し、表示されたページでこのボタンを使用する必要があります。

ステップ 6 [保存 (Save)] をクリックします。

管理者の高度なロール設定

高度なロール設定を使用すると、カスタムロールの権限をより詳細なレベルで編集できます。[エンドユーザの設定 (End User configuration)] ウィンドウと [アプリケーションユーザの設定 (Application User configuration)] ウィンドウで、次のキー設定を編集する管理者の機能を制御できます。

- ユーザ ランクの編集
- アクセス コントロール グループの割り当ての編集
- 新規ユーザの追加
- ユーザパスワードの編集

手順

ステップ 1 Cisco Unified CM Administration で、[ユーザ管理 (User Management)] > [ユーザ設定 (User Settings)] > [ロール (Role)] を選択します。

ステップ 2 [検索 (Find)] をクリックして、カスタムロールを選択します。

ステップ 3 [関連リンク (Related Links)] で、[詳細なロール設定 (Advanced Role Configuration)] を選択し、[Go (移動)] をクリックします。

ステップ 4 [リソース (Resource)] Web ページで、[アプリケーション ユーザ (Application User)] Web ページまたは [ユーザ (User)] Web ページを選択します。

ステップ 5 設定の編集フィールドおよびその設定についてのヘルプは、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。

アクセス制御グループの作成

新しいアクセス制御グループを作成する必要がある場合に、この手順を使用します。必要なロールとアクセス権限を持つ標準のグループがない場合に、この方法を使用できます。カスタマイズされたグループを作成する方法には、次の2つがあります。

- **[新規追加 (Add New)]** ボタンを使用して、scatch から新しいアクセス制御グループを作成および設定します。
- 必要な内容に近いロールが既存のグループ割り当てられている場合は、**[コピー (Copy)]** ボタンを使用します。既存のグループから、新しい編集可能なグループに設定をコピーできます。

手順

ステップ 1 Cisco Unified CM Administration で、**[ユーザ管理 (User Management)]** > **[ユーザ設定 (User Settings)]** > **[アクセス制御グループ (Access Control Group)]** を選択します。

ステップ 2 次のいずれかを実行します。

- 新しいグループを最初から作成するには、**[新規追加 (Add New)]** をクリックします。
- 既存のグループから設定をコピーするには、**[検索 (Find)]** をクリックして、既存のアクセス制御グループを開きます。**[コピー (Copy)]** をクリックして、新しいグループの名前を入力します。**[OK]** をクリックします。

ステップ 3 **[名前 (Name)]** にアクセス制御グループの名前を入力します。

ステップ 4 **[ユーザで利用できるユーザランク (Available for Users with User Rank as)]** ドロップダウンから、このグループに割り当てる、ユーザの最低ランクを選択します。デフォルトのユーザランクは 1 です。

ステップ 5 **[保存 (Save)]** をクリックします。

ステップ 6 アクセス制御グループにロールを割り当てます。選択したロールは、グループのメンバーに割り当てられます。

- a) **[関連リンク (Related Links)]** から、**[アクセス制御グループへの権限の割り当て (Assign Roles to Access Control Group)]** を選択して **[実行 (Go)]** をクリックします。
- b) **[検索 (Find)]** をクリックして、既存のロールを検索します。
- c) 追加するロールをオンにして、**[選択の追加 (add Selected)]** をクリックします。
- d) **[保存 (Save)]** をクリックします。

次のタスク

[アクセス制御グループへのユーザの割り当て \(29 ページ\)](#)

アクセス制御グループへのユーザの割り当て

標準またはカスタムのアクセス制御グループに対してユーザを追加または削除します。



(注) ユーザのランクがアクセス制御グループの最低ユーザランクと同じかそれより上のユーザのみを追加できます。



(注) 会社の LDAP ディレクトリから新しいユーザを同期し、ランク階層とアクセスコントロールグループが適切な権限で作成されている場合、LDAP同期の一部としてグループを同期されたユーザに割り当てることができます。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』を参照してください。

手順

- ステップ 1** [ユーザ管理 (User Management)] > [ユーザ設定 (User Settings)] > [アクセス制御グループ (Access Control Group)] を選択します。
[アクセス制御グループの検索と一覧表示 (Find and List Access Control Groups)] ウィンドウが表示されます。
- ステップ 2** [検索 (Find)] をクリックして、ユーザリストを更新するアクセス制御グループを選択します。
- ステップ 3** [ユーザで利用できるユーザランク (Available for Users with User Rank as)] ドロップダウンから、このグループに割り当てるために必要なユーザのランク要件を選択します。
- ステップ 4** [ユーザ] セクションで、[検索 (Find)] をクリックして、ユーザリストを表示します。
- ステップ 5** エンドユーザまたはアプリケーションユーザをアクセス制御グループに追加するには、次の手順を実行します。
 - a) [エンドユーザをアクセス制御グループに追加 (Add End Users to Access Control Group)] または [アプリケーションユーザをアクセス制御グループに追加 (Add App Users to Access Control Group)] をクリックします。
 - b) 追加するユーザを選択します。
 - c) [選択項目の追加 (Add Selected)] をクリックします。
- ステップ 6** アクセス制御グループからユーザを削除するには、次の手順を実行します。
 - a) 削除するユーザを選択します。
 - b) [選択項目の削除 (Delete Selected)] をクリックします。
- ステップ 7** [保存 (Save)] をクリックします。

アクセス制御グループの重複する特権ポリシーの設定

Cisco Unified Communications Manager がアクセス制御グループの割り当てにより発生する可能性がある、ユーザ権限の重複を処理する方法を設定します。これにより、エンドユーザが複数のアクセス制御グループに割り当てられ、ルールや権限の設定に不整合が生まれる状況に対処できます。

手順

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

ステップ 2 [ユーザ管理パラメータ (User Management Parameters)] で、[重複したユーザグループとロールの実質的なアクセス権 (Effective Access Privileges For Overlapping User Groups and Roles)] に次のいずれかの値を設定します。

- [最大 (Maximum)] —実質的な権限は、重複したすべてのアクセス制御グループの最大限の権限になります。これがデフォルトのオプションです。
- [最小 (Minimum)] —実質的な権限は、重複したすべてのアクセス制御グループの最小限の権限になります。

ステップ 3 [保存 (Save)] をクリックします。

ユーザ権限レポートの表示

既存のエンドユーザや既存のアプリケーションユーザのユーザ権限レポートを表示するには、次の手順を実行します。ユーザ権限レポートは、エンドユーザまたはアプリケーションユーザに割り当てられたアクセス制御グループ、ルール、およびアクセス権限が表示されます。

手順

ステップ 1 Cisco Unified CM の管理で、次の手順のいずれかを実行します。

- エンドユーザの場合は、[ユーザの管理 (User Management)] > [エンドユーザ (End User)] を選択します。
- アプリケーションユーザの場合は、[ユーザの管理 (User Management)] > [アプリケーションユーザ (Application User)] を選択します。

ステップ 2 [検索 (Find)] をクリックして、アクセス権限を表示するユーザを選択します。

ステップ 3 [関連リンク (Related Links)] ドロップダウンリストから [ユーザ権限レポート (User Privilege Report)] を選択し、[移動 (Go)] をクリックします。
[ユーザ権限 (User Privilege)] ウィンドウが表示されます。

カスタム ヘルプ デスク ロールの作成タスク フロー

企業によっては、ヘルプデスク担当者に特定の管理タスクを実行できる権限を与える必要があると考えている場合があります。このタスクフロー内の手順に従って、電話機の追加やエンドユーザの追加などのタスクをヘルプデスク チームのメンバーが実行できるようにする、ヘルプデスク チームのメンバー用のロールとアクセス コントロール グループを設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	カスタム ヘルプ デスク 権限の作成 (31 ページ)	ヘルプ デスク チームのメンバーのカスタム ロールを作成し、新しい電話機の追加や新しいユーザの追加などの項目のロール権限を割り当てます。
ステップ 2	カスタム ヘルプ デスク アクセス コントロール グループの作成 (32 ページ)	ヘルプ デスク ロール用の新しいアクセス コントロール グループを作成します。
ステップ 3	アクセス コントロール グループへのヘルプ デスク ロールの割り当て (32 ページ)	ヘルプ デスク アクセス コントロール グループにヘルプ デスク ロールを割り当てます。このアクセス コントロール グループに割り当てられたユーザには、ヘルプ デスク ロールの権限が割り当てられます。
ステップ 4	アクセス コントロール グループへのヘルプ デスク メンバーの割り当て (33 ページ)	カスタム ヘルプ デスク ロールの権限をヘルプ デスク チームのメンバーに割り当てます。

カスタム ヘルプ デスク 権限の作成

この手順を実行して、組織内のヘルプ デスク メンバーに割り当てることができるカスタム ヘルプ デスク 権限を作成します。

手順

- ステップ 1 [Cisco Unified CM の管理 (Cisco Unified Communications Manager Administration)] で、[ユーザ管理 (User Management)] > [ユーザ設定 (User Settings)] > [権限 (Role)] をクリックします。
- ステップ 2 [新規追加 (Add New)] をクリックします。
- ステップ 3 [アプリケーション (Application)] ドロップダウンリストから、この権限に割り当てるアプリケーションを選択します。たとえば、[Cisco CallManager Administration] を選択します。
- ステップ 4 [次へ (Next)] をクリックします。

- ステップ 5** 新しい権限の [名前 (Name)] を入力します。たとえば、**Help Desk** です。
- ステップ 6** [読み込みおよび更新権限 (Read and Update Privileges)] の下で、ヘルプ デスク ユーザに割り当てる権限を選択します。たとえば、ヘルプ デスク メンバーがユーザおよび電話を追加できるようにする場合は、[ユーザ (User)] Web ページと [電話 (Phone)] Web ページの [読み込み (Read)] および [更新 (Update)] チェック ボックスをオンにします。
- ステップ 7** [保存 (Save)] をクリックします。

次のタスク

[カスタム ヘルプ デスク アクセス コントロール グループの作成 \(32 ページ\)](#)

カスタム ヘルプ デスク アクセス コントロール グループの作成

始める前に

[カスタム ヘルプ デスク 権限の作成 \(31 ページ\)](#)

手順

- ステップ 1** Cisco Unified CM の管理で、[ユーザ管理 (User Management)] > [ユーザ設定 (User Settings)] > [アクセス コントロール グループ (Access Control Group)] 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** アクセス コントロール グループの名前を入力します。たとえば、「**Help_Desk**」と入力します。
- ステップ 4** [保存 (Save)] をクリックします。

次のタスク

[アクセス コントロール グループへのヘルプ デスク ロールの割り当て \(32 ページ\)](#)

アクセス コントロール グループへのヘルプ デスク ロールの割り当て

次の手順を実行して、ヘルプ デスク ロールからの権限を持つヘルプ デスク アクセス コントロール グループを設定します。

始める前に

[カスタム ヘルプ デスク アクセス コントロール グループの作成 \(32 ページ\)](#)

手順

- ステップ 1 Cisco Unified CM の管理で、[ユーザ管理 (User Management)] > [ユーザ設定 (User Settings)] > [アクセスコントロールグループ (Access Control Group)] を選択します。
- ステップ 2 [検索 (Find)] をクリックし、ヘルプデスク用に作成したアクセスコントロールグループを選択します。
[アクセスコントロールグループの設定 (Access Control Group Configuration)] ウィンドウが開きます。
- ステップ 3 [関連リンク (Related Links)] ドロップダウンリストボックスで、[アクセスコントロールグループに権限を割り当て (Assign Role to Access Control Group)] オプションを選択し、[移動 (Go)] をクリックします。
[権限の検索/一覧表示 (Find and List Roles)] ポップアップが表示されます。
- ステップ 4 [グループに権限を割り当て (Assign Role to Group)] ボタンをクリックします。
- ステップ 5 [検索 (Find)] をクリックし、ヘルプデスクロールを選択します。
- ステップ 6 [選択項目の追加 (Add Selected)] をクリックします。
- ステップ 7 [保存 (Save)] をクリックします。

次のタスク

[アクセスコントロールグループへのヘルプデスクメンバーの割り当て \(33 ページ\)](#)

アクセスコントロールグループへのヘルプデスクメンバーの割り当て

始める前に

[アクセスコントロールグループへのヘルプデスクロールの割り当て \(32 ページ\)](#)

手順

- ステップ 1 Cisco Unified CM の管理で、[ユーザ管理 (User Management)] > [ユーザ設定 (User Settings)] > [アクセスコントロールグループ (Access Control Group)] を選択します。
- ステップ 2 [検索 (Find)] をクリックし、作成したカスタムヘルプデスクアクセスコントロールグループを選択します。
- ステップ 3 次のいずれかの手順を実行します。
 - ヘルプデスクチームのメンバーがエンドユーザとして設定されている場合は、[グループにエンドユーザを追加 (Add End Users to Group)] をクリックします。
 - ヘルプデスクチームのメンバーがアプリケーションユーザとして設定されている場合は、[グループにアプリケーションユーザを追加 (Add App Users to Group)] をクリックします。
- ステップ 4 [検索 (Find)] をクリックし、ヘルプデスクユーザを選択します。

ステップ5 [選択項目の追加 (Add Selected)] をクリックします。

ステップ6 [保存 (Save)] をクリックします。

Cisco Unified Communications Manager が、作成したカスタム ヘルプ デスク ロールの権限をヘルプ デスク チームのメンバーに割り当てます。

アクセスコントロールグループの削除

アクセスコントロールグループ全体を削除するには、次の手順を使用します。

始める前に

アクセスコントロールグループを削除すると、Cisco Unified Communications Manager がデータベースからすべてのアクセスコントロールグループデータを削除します。アクセスコントロールグループを使用しているロールが判明していることを確認します。

手順

ステップ1 [ユーザ管理 (User Management)] > [ユーザ設定 (User Settings)] > [アクセスコントロールグループ (Access Control Group)] の順に選択します。

[アクセス制御グループの検索と一覧表示 (Find and List Access Control Groups)] ウィンドウが表示されます。

ステップ2 削除するアクセスコントロールグループを検索します。

ステップ3 削除するアクセスポイントグループの名前をクリックします。

選択したアクセスコントロールグループが表示されます。このアクセスコントロールグループ内のユーザがアルファベット順に一覧表示されます。

ステップ4 アクセスコントロールグループ全体を削除するには、[削除 (Delete)] をクリックします。

アクセスコントロールグループを削除すると元に戻せないことを警告するダイアログボックスが表示されます。

ステップ5 アクセスコントロールグループを削除するには、[OK] をクリックします。アクションをキャンセルするには、[キャンセル (Cancel)] をクリックします。[OK] をクリックすると、Cisco Unified Communications Manager がデータベースからアクセスコントロールグループを削除します。

既存の OAuth 更新トークンの取り消し

既存の OAuth 更新トークンを取り消すには、AXL API を使用します。たとえば、ある従業員が退社した場合、この API を使用してその従業員の現在の更新トークンを取り消し、その従業員が新しいアクセストークンを取得したり、企業アカウントへログインできないようにするこ

とができます。APIは、AXLクレデンシャルで保護されているRESTベースのAPIです。任意のコマンドライン ツールを使用してAPIを呼び出すことができます。次のコマンドは、更新トークンを取り消すために使用できるcURLコマンドの例を示しています。

```
curl -k -u "admin:password" https://<UCMaddress:8443/ssosp/token/ revoke?user_id=<end_user>
```

引数の説明

- admin:password は、Cisco Unified Communications Manager の管理者アカウントのログイン ID とパスワードです。
- UCMaddress は、Cisco Unified Communications Manager のパブリッシャ ノードの FQDN または IP アドレスです。
- end_user は、更新トークンを取り消すユーザのユーザ ID です。

非アクティブなユーザアカウントの無効化

Cisco Database Layer Monitor サービスを使用して非アクティブなユーザアカウントを無効にするには、次の手順を実行します。

Cisco Database Layer Monitor は、指定日数内に Cisco Unified Communications Manager にログインしていない場合、スケジュールされたメンテナンス タスク時にユーザアカウントステータスを非アクティブに変更します。無効にされたユーザは、その後の監査ログで自動的に監査対象になります。

始める前に

Cisco Database Layer Monitor サービスで選択したサーバの [メンテナンス時間 (Maintenance Time)] を入力します ([システム (System)] > [サービスパラメータ (Service Parameters)])。

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)] の順に選択します。
- ステップ 2** [サーバ (Server)] ドロップダウンリスト ボックスからサーバを選択します。
- ステップ 3** [サービス (Service)] ドロップダウンリスト ボックスから [Cisco Database Layer Monitor] パラメータを選択します。
- ステップ 4** [Advanced] をクリックします。
- ステップ 5** [この期間未使用のユーザアカウントを無効化する (Disable User Accounts unused for (days))] フィールドに、日数を入力します。たとえば、90とします。システムはこの入力された値を、非アクティブとしてアカウントの状態を宣言するためのしきい値として使用します。自動無効化をオフにするには、値を 0 と入力します。

(注) これは必須フィールドです。デフォルトおよび最小値は 0 で、単位は日数です。

ステップ 6 [保存 (Save)] をクリックします。

非アクティブなまま設定された日数 (たとえば 90 日間) が経過すると、ユーザは無効になります。監査ログにエントリが作成され、次のメッセージが表示されます。「<userID> ユーザは非アクティブとマークされています (<userID> user is marked inactive) 」。

リモートアカウントの設定

シスコサポートがトラブルシューティングのためにご使用のシステムに一時的にアクセスできるように、Unified Communications Manager でリモートアカウントを設定します。

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)] で、[サービス (Services)] > [リモートサポート (Remote Support)] を選択します。

ステップ 2 [アカウント名 (Account Name)] フィールドに、リモートアカウントの名前を入力します。

ステップ 3 [アカウントの有効期限 (Account Duration)] フィールドに、アカウントの有効期限を日数で入力します。

ステップ 4 [保存 (Save)] をクリックします。

システムは、暗号化パスワードを生成します。

ステップ 5 シスコのサポート担当者に連絡して、リモートサポートアカウント名とパスワードを提供します。

標準ロールとアクセス制御グループ

次の表は、Cisco Unified Communications Manager にあらかじめ設定されている標準権限およびアクセス制御グループの概要です。標準権限が持つ特権はデフォルトで設定されています。また、標準権限に関連付けられたアクセス制御グループも、デフォルトで設定されています。

標準権限、および標準権限に関連付けられたアクセス制御グループの両方で、特権または権限の割り当てを編集できません。

表 3: 標準権限、特権 およびアクセス制御グループ

標準権限	権限に対する特権およびリソース	関連付けられた標準アクセス制御グループ
標準 AXL API アクセス	AXL データベース API へのアクセスを許可します。	[標準 CCM スーパーユーザー (Standard CCM Super Users)]

標準権限	権限に対する特権およびリソース	関連付けられた標準アクセス制御グループ
標準AXL APIユーザー	AXL APIを実行するログイン権限を付与します。	
標準 AXL 読み取り専用 API アクセス	AXL 読み取り専用 API (API の一覧表示、API の取得、SQL Query API の実行) の実行をデフォルトで許可します。	
標準管理 Rep Tool 管理	Cisco Unified Communications Manager CDR Analysis and Reporting (CAR) の表示および設定が可能になります。	標準 CAR 管理ユーザー、標準 CCM スーパー ユーザー
標準監査ログ管理	<p>監査ロギング機能の次のタスクを実行できます。</p> <ul style="list-style-type: none"> • Cisco Unified Serviceability の [監査ログ設定 (Audit Log Configuration)] ウィンドウでの、監査ロギングの表示および設定 • Cisco Unified Serviceability でのトレースの表示と設定、および Real-Time Monitoring Tool の監査ログ機能向けトレースの収集 • Cisco Unified Serviceability での Cisco Audit Event Service の表示、開始、停止 • RTMT での、関連付けられたアラートの表示および更新 	標準監査ユーザー
標準 CCM 管理ユーザー	Cisco Unified Communications Manager Administration へのログイン権限を付与します。	標準 CCM 管理ユーザー、標準 CCM ゲートウェイ管理、標準 CCM 電話管理、標準 CCM 読み取り専用、標準 CCM サーバー モニタリング、標準 CCM スーパー ユーザー、標準 CCM サーバーメンテナンス、標準 パケット スニファ ユーザー
[標準CCMエンドユーザー (Standard CCM End Users)]	Cisco Unified Communications セルフケアポータルにログインする権限をエンドユーザーに付与します。	[標準CCMエンドユーザー (Standard CCM End Users)]

標準権限	権限に対する特権およびリソース	関連付けられた標準アクセス制御グループ
標準 CCM 機能管理	<p>Cisco Unified Communications Manager Administration で、次のタスクを実行できます。</p> <ul style="list-style-type: none"> • 一括管理ツールによる次の項目の表示、削除、挿入： <ul style="list-style-type: none"> • クライアント関連のコードと強制承認コード • コール ピックアップ グループ • Cisco Unified Communications Manager Administration で、の次の項目を表示、設定できます。 <ul style="list-style-type: none"> • クライアント関連のコードと強制承認コード • コール パーク • コール ピックアップ • ミートミーの番号またはパターン • メッセージ受信 • Cisco Unified IP Phone サービス • ボイスメールパイロット、ボイスメールポートウィザード、ボイスメールポート、ボイスメールプロフィール 	[標準CCMサーバーメンテナンス (Standard CCM Server Maintenance)]
標準 CCM ゲートウェイ管理	<p>Cisco Unified Communications Manager Administration で、次のタスクを実行できます。</p> <ul style="list-style-type: none"> • 一括管理ツールによるゲートウェイテンプレートの表示および設定 • ゲートキーパー、ゲートウェイ、およびトランクの表示および設定 	標準 CCM ゲートウェイ管理

標準権限	権限に対する特権およびリソース	関連付けられた標準アクセス制御グループ
標準 CCM 電話管理	<p>Cisco Unified Communications Manager Administration で、次のタスクを実行できます。</p> <ul style="list-style-type: none"> • 一括管理ツールによる電話の表示とエクスポート • 一括管理ツールによるユーザーデバイスプロファイルの表示と挿入 • Cisco Unified Communications Manager Administration で、次の項目を表示および設定できます。 <ul style="list-style-type: none"> • BLF 短縮ダイヤル • CTI ルート ポイント • デフォルトデバイスプロファイルまたはデフォルト プロファイル • 電話番号、および回線の状態 • ファームウェア ロード情報 • 電話ボタンテンプレートまたはソフトキー テンプレート • 電話機 • [電話の設定 (Phone Configuration)] ウィンドウの [ボタン項目を変更 (Modify Button Items)] をクリックすることによる、特定の電話に対する電話ボタンの情報の並べ替え 	標準 CCM 電話管理

標準権限	権限に対する特権およびリソース	関連付けられた標準アクセス制御グループ
標準 CCM ルートプラン管理	<p>Cisco Unified Communications Manager Administration で、次のタスクを実行できます。</p> <ul style="list-style-type: none"> • アプリケーションダイヤルルールの表示および設定 • コーリングサーチスペースおよびパーティションの表示および設定 • ダイヤルルールパターンを含むダイヤルルールの表示および設定 • ハントリスト、ハントパイロット、回線グループの表示および設定 • ルートフィルタ、ルートグループ、ルートハントリスト、ルートリスト、ルートパターン、ルートプランレポートの表示および設定 • 時間帯およびスケジュールの表示および設定 • トランスレーションパターンの表示および設定 	

標準権限	権限に対する特権およびリソース	関連付けられた標準アクセス制御グループ
標準 CCM サービス管理	<p>Cisco Unified Communications Manager Administration で、次のタスクを実行できます。</p> <ul style="list-style-type: none"> • 次の項目を表示および設定できます。 <ul style="list-style-type: none"> • アナンシエータ、会議ブリッジ、トランスコーダ • オーディオ ソースおよび MOH サーバー • メディアリソースグループおよびメディアリソースグループリスト • Media Termination Point; メディアターミネーションポイント • Cisco Unified Communications Manager Assistant ウィザード • 一括管理ツールの [マネージャの削除 (Delete Managers)]、[マネージャ/アシスタントの削除 (Delete Managers/Assistants)]および [マネージャ/アシスタントの挿入 (Insert Managers/Assistants)] ウィンドウでの表示および設定ができます。 	[標準CCMサーバーメンテナンス (Standard CCM Server Maintenance)]

標準権限	権限に対する特権およびリソース	関連付けられた標準アクセス制御グループ
標準 CCM システム管理	<p>Cisco Unified Communications Manager Administration で、次のタスクを実行できます。</p> <ul style="list-style-type: none"> • 次の項目を表示および設定できます。 <ul style="list-style-type: none"> • 代替ルーティング (AAR) グループの自動化 • Cisco Unified Communications Manager (Cisco Unified CM) および Cisco Unified Communications Manager グループ • 日時グループ • デバイス デフォルト • デバイス プール • エンタープライズ パラメータ • エンタープライズ電話の設定 • ロケーション • Network Time Protocol (NTP) サーバー • プラグイン • Skinny Call Control Protocol (SCCP) または Session Initiation Protocol (SIP) を実行する電話用のセキュリティプロファイル、SIP トランク用のセキュリティプロファイル • Survivable Remote Site Telephony (SRST) の参照 • サーバー • 一括管理ツールの、[ジョブスケジューラ (Job Scheduler)] ウィンドウでの表示と設定 	標準CCMサーバメンテナンス (Standard CCM Server Maintenance)

標準権限	権限に対する特権およびリソース	関連付けられた標準アクセス制御グループ
標準 CCM ユーザー権限管理	Cisco Unified Communications Manager Administration で、アプリケーション ユーザの表示および設定を実行できます。	
標準CCMADMIN管理 (Standard CCMADMIN Administration)	CCMAdmin システムのすべての面を利用できます。	
標準CCMADMIN管理 (Standard CCMADMIN Administration)	Cisco Unified Communications Manager Administration および一括管理ツールのすべての項目を表示および設定できます。	[標準CCMスーパーユーザー (Standard CCM Super Users)]
標準CCMADMIN管理 (Standard CCMADMIN Administration)	Dialed Number Analyzer の情報を表示および設定できます。	
標準CCMADMIN読み取り専用 (Standard CCMADMIN Read Only)	すべての CCMAdmin リソースの読み取りを許可します。	
標準CCMADMIN読み取り専用 (Standard CCMADMIN Read Only)	Cisco Unified Communications Manager Administration および一括管理ツールの項目を表示できます。	標準 CCM ゲートウェイ管理、標準 CCM 電話管理、標準 CCM 読み取り専用、標準 CCM サーバー メンテナンス、標準 CCM サーバー モニタリング
標準CCMADMIN読み取り専用 (Standard CCMADMIN Read Only)	Dialed Number Analyzer で、ルーティング設定の分析ができます。	
標準 CCMUSER 管理	Cisco Unified Communications セルフケアポータルへのアクセスを許可します。	標準CCMエンドユーザ (Standard CCM End Users)
標準CTI通話モニタリング許可	CTIアプリケーションまたはデバイスでコールをモニターできます。	標準CTI通話モニタリング許可

標準権限	権限に対する特権およびリソース	関連付けられた標準アクセス制御グループ
標準CTIコールパークモニタリング許可	CTIアプリケーションまたはデバイスでコールパークを使用できます。 重要 開通している回線およびパーク回線の最大数は 65,000 を超えてはなりません。 合計が 65,000 を超える場合は、アプリケーションユーザから Standard CTI Allow Call Park Monitoring ロールを削除するか、設定されているパーク回線の数を減らします。	標準 CTI コールパーク モニタリング許可
標準CTI通話録音許可	CTIアプリケーション/デバイスで通話を録音できます。	標準 CTI 通話録音許可
標準CTI発信者番号の変更許可	CTIアプリケーションが発信者番号を通話中に変更できます。	標準 CTI 発信者番号の変更許可
標準CTIによるすべてのデバイスの制御	CTI で制御可能なすべてのデバイスを制御できます。	標準 CTI によるすべてのデバイスの制御
標準CTI接続された転送と会議をサポートする電話の制御許可	接続された転送および会議をサポートするすべての CTI デバイスを制御できます。	標準 CTI 接続された転送と会議をサポートする電話の制御許可
標準 CTI ロールオーバーモードをサポートする電話の制御許可	ロールオーバーモードをサポートするすべての CTI デバイスを制御できます。	標準 CTI ロールオーバーモードをサポートする電話の制御許可
標準 CTI SRTP 重要素材の受信許可	CTIアプリケーションが、SRTP を使用する重要な素材にアクセスしたり、その素材を配信したりできるようにします。	標準 CTI SRTP 重要素材の受信許可
標準 CTI 対応	CTIアプリケーションの制御を可能にします。	標準 CTI 対応
標準CTIセキュア接続	Cisco Unified Communications Manager へのセキュアな CTI 接続が可能になります。	標準 CTI セキュア接続
標準CUREporting (Standard CUREporting)	アプリケーションユーザが、さまざまなソースからレポートを作成できます。	

標準権限	権限に対する特権およびリソース	関連付けられた標準アクセス制御グループ
標準CUReporting (Standard CUReporting)	Cisco Unified Reporting での、レポートの表示、ダウンロード、作成、およびアップロードができます。	標準 CCM 管理ユーザー、標準 CCM スーパーユーザー
標準 EM 認証プロキシ権限	アプリケーションで使用する Cisco Extension Mobility (EM) の認証権限を管理します。この権限は、(Cisco Unified Communications Manager Assistant や Cisco Web Dialer などの) Cisco Extension Mobility と対話するすべてのアプリケーションユーザに必要です。	標準 CCM スーパーユーザー、標準 EM 認証プロキシ権限
標準パケットスニッフィング	Cisco Unified Communications Manager の管理にアクセスし、パケットスニッフィング (キャプチャ) ができます。	標準パケットスニファユーザー
標準 RealtimeAndTraceCollection (Standard RealtimeAndTraceCollection)	Cisco Unified Serviceability および Real-Time Monitoring Tool にアクセスし、次の項目を表示および使用できます。 <ul style="list-style-type: none"> • Simple Object Access Protocol (SOAP) Serviceability AXL API • SOAP コール レコード API • SOAP 診断ポータル (Analysis Manager) データベース サービス • 監査ログ機能のトレースの設定 • トレース収集などの、Real-Time Monitoring Tool の設定 	標準 RealtimeAndTraceCollection (Standard RealtimeAndTraceCollection)

標準権限	権限に対する特権およびリソース	関連付けられた標準アクセス制御グループ
標準 SERVICEABILITY	<p>Cisco Unified Serviceability または Real-Time Monitoring Tool で、次のウィンドウを表示および設定できます。</p> <ul style="list-style-type: none"> • [アラーム設定およびアラーム定義 (Alarm Configuration and Alarm Definitions)] (Cisco Unified Serviceability) • [監査トレース (Audit Trace)] (読み取りおよび表示のみ可能なマークが付けられています) • SNMP 関連のウィンドウ (Cisco Unified Serviceability) • [トレースの設定 (Trace Configuration)] および [トレース設定のトラブルシューティング (Troubleshooting of Trace Configuration)] (Cisco Unified Serviceability) <p>)</p> <ul style="list-style-type: none"> • ログパーティションのモニタリング • [アラートの設定 (Alert Configuration)] (RTMT) 、 [プロファイルの設定 (Profile Configuration)] (RTMT) 、 および [トレース収集 (Trace Collection)] (RTMT) <p>SOAP Serviceability AXL API、SOAP Call Record API、および SOAP 診断ポータル (Analysis Manager) データベース サービスを表示および使用できます。</p> <p>SOAP コールレコード API については、RTMT Analysis Manager Call Record の権限が、このリソースを介して制御されます。</p> <p>SOAP 診断ポータルデータベースサービスについては、RTMT Analysis Manager Hosting Database アクセスが、このリソースを介して制御されます。</p>	標準 CCM サーバー モニタリング、標準 CCM スーパー ユーザー

標準権限	権限に対する特権およびリソース	関連付けられた標準アクセス制御グループ
標準 SERVICEABILITY 管理	有用性の管理者は、Cisco Unified Communications Manager の管理に表示されるプラグインウィンドウにアクセスでき、このウィンドウからプラグインをダウンロードできます。	
標準 SERVICEABILITY 管理 (Standard SERVICEABILITY Administration)	Dialed Number Analyzer の有用性をすべての面で管理できます。	
標準 SERVICEABILITY 管理 (Standard SERVICEABILITY Administration)	Cisco Unified Serviceability および Real-Time Monitoring Tool のすべてのウィンドウを表示および設定できます ([監査トレース (Audit Trace)] では表示のみ可能です)。 すべての SOAP Serviceability AXL API を表示および使用できます。	
標準 SERVICEABILITY 読み取り専用 (Standard SERVICEABILITY Read Only)	Dialed Number Analyzer のコンポーネントで使用する有用性に関するすべてのデータを表示できます。	標準 CCM 読み取り専用
標準 SERVICEABILITY 読み取り専用 (Standard SERVICEABILITY Read Only)	Cisco Unified Serviceability および Real-Time Monitoring Tool で、設定を表示できます。 (標準監査ログ管理の権限により表示される監査設定ウィンドウは除きます) SOAP Serviceability AXL API、SOAP Call Record API、および SOAP 診断ポータル (Analysis Manager) データベース サービスをすべて表示できます。	
標準システムサービス管理	Cisco Unified Serviceability で、サービスを表示、アクティベート、開始、および停止できます。	
標準 SSO 設定管理	SAML SSO の設定をすべての面で管理できます。	
標準機密アクセスレベル ユーザー	すべての機密アクセス レベル ページにアクセスできます。	標準 Cisco Call Manager 管理

標準権限	権限に対する特権およびリソース	関連付けられた標準アクセス制御グループ
標準CCMADMIN管理	CCMAdmin システムをすべての面で管理できます。	標準 Cisco Unified CM IM and Presence の管理
標準CCMADMIN読み取り専用 (Standard CCMADMIN Read Only)	すべての CCMAdmin リソースの読み取りを許可します。	標準 Cisco Unified CM IM and Presence の管理
標準CUReporting (Standard CUReporting)	アプリケーションユーザーが、さまざまなソースからレポートを作成できます。	標準 Cisco Unified CM IM & Presence のレポート ティング



第 5 章

エンドユーザの管理

- [エンドユーザの概要 \(49 ページ\)](#)
- [エンドユーザ管理タスク \(49 ページ\)](#)

エンドユーザの概要

稼働中のシステムを管理する際に、システム内に設定済みのエンドユーザのリストを更新しなければならない場合があります。次の作業が含まれます。

- 新しいユーザの設定
- 新しいエンドユーザの電話機の設定
- エンドユーザのパスワードまたは PIN の変更
- IM and Presence Service に対するエンドユーザの有効化

Cisco Unified CM の管理の [エンドユーザの設定 (End User Configuration)] ウィンドウで、Unified CM エンドユーザに関する情報を追加、検索、表示、保守できます。また、[ユーザ/電話のクイック追加 (Quick User/Phone Add)] ウィンドウを使用して、新規エンドユーザとそのエンドユーザの新規電話を迅速に設定することもできます。

エンドユーザ管理タスク

手順

	コマンドまたはアクション	目的
ステップ 1	ユーザテンプレートの設定 (50 ページ)	ユニバーサル回線テンプレートとデバイステンプレートを含むユーザプロファイルまたは機能グループテンプレートを使用してシステムを設定していない場合は、次のタスクを実行してセットアップします。

	コマンドまたはアクション	目的
		これらのテンプレートを新しいエンドユーザに適用することにより、新しいユーザと電話機を簡単に設定できます。
ステップ 2	<p>次の方法のいずれかを使用して新しいエンドユーザを追加します</p> <ul style="list-style-type: none"> • LDAP からのエンドユーザのインポート (56 ページ) • エンドユーザの手動追加 (57 ページ) 	<p>システムが設定済みであり会社の LDAP ディレクトリと同期している場合は、新しいエンドユーザを LDAP から直接インポートできます。</p> <p>まだ設定していない場合は、エンドユーザを手動で追加して設定できます。</p>
ステップ 3	<p>次のタスクのどちらかを実行することにより、新しいまたは既存のエンドユーザに電話機を割り当てます。</p> <ul style="list-style-type: none"> • エンドユーザ用の新しい電話機の追加 (58 ページ) • エンドユーザへの既存の電話機の移動 (59 ページ) 	<p>「新しい電話機の追加」手順に従い、ユニバーサルデバイステンプレートの設定を使用して、エンドユーザの新しい電話機を設定できます。</p> <p>また、「移動」手順に従って、すでに設定済みの既存の電話機を割り当てることもできます。</p>
ステップ 4	エンドユーザ PIN の変更 (60 ページ)	(オプション) Cisco Unified Communications Manager Administration でエンドユーザの PIN を変更する。
ステップ 5	エンドユーザパスワードの変更 (60 ページ)	(オプション) Cisco Unified Communications Manager Administration でエンドユーザのパスワードを変更する。
ステップ 6	Cisco Unity Connection ボイスメールボックスの作成 (61 ページ)	(オプション) Cisco Unified Communications Manager Administration で個別の Cisco Unity Connection ボイスメールボックスを作成する。

ユーザテンプレートの設定

次のタスクを実行して、ユーザプロファイルおよび機能グループテンプレートを設定します。新しいエンドユーザを追加したら、回線およびデバイス設定を使用してすばやくエンドユーザを設定し、エンドユーザの電話を設定できます。

手順

	コマンドまたはアクション	目的
ステップ 1	ユニバーサル回線テンプレートの設定 (51 ページ)	電話番号に一般的に適用される共通設定を使用して、ユニバーサル回線テンプレートを設定します。
ステップ 2	ユニバーサルデバイステンプレートの設定 (52 ページ)	電話に一般的に適用される共通設定を使用して、ユニバーサルデバイステンプレートを設定します。
ステップ 3	ユーザプロファイルの設定 (53 ページ)	ユニバーサル回線テンプレートとユニバーサルデバイステンプレートをユーザプロファイルに割り当てます。セルフプロビジョニング機能を設定している場合は、このプロファイルを使用するユーザに対してセルフプロビジョニングを有効化できます。
ステップ 4	機能グループテンプレートの設定 (55 ページ)	機能グループテンプレートにユーザプロファイルを割り当てます。LDAP同期ユーザの場合は、機能グループテンプレートによってユーザプロファイル設定がエンドユーザに関連付けられます。

ユニバーサル回線テンプレートの設定

ユニバーサル回線テンプレートを使用すると、新しく割り当てられたディレクトリ番号に共通の設定を簡単に適用できます。さまざまなユーザグループのニーズに合わせて、異なるテンプレートを設定します。

手順

- ステップ 1 Cisco Unified CM Administration で、**[ユーザ管理 (User Management)]** > **[ユーザ/電話の追加 (User/Phone Add)]** > **[ユニバーサル回線テンプレート (Universal Line Template)]** 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 **[ユニバーサル回線テンプレートの設定 (Universal Line Template Configuration)]** ウィンドウで各フィールドを設定します。フィールドとその設定オプションの詳細については、オンラインヘルプを参照してください。
- ステップ 4 代替番号を使用したグローバルダイヤルプランレプリケーションを展開する場合は、**[エンタープライズ代替番号 (Enterprise Alternate Number)]** セクションと **[+E.164代替番号 (+E.164 Alternate Number)]** セクションを展開して、次の手順を実行します。

- a) [エンタープライズ代替番号の追加 (Add Enterprise Alternate Number)] ボタンまたは [+E.164 代替番号の追加 (Add +E.164 Alternate Number)] ボタンのいずれか、または両方をクリックします。
- b) 代替番号への割り当てに使用する [番号マスク (Number Mask)] を追加します。たとえば、4桁の内線番号では、エンタープライズ番号マスクとして 5XXXX を使用し、+E.164 代替番号マスクとして 1972555XXXX を使用することが考えられます。
- c) 代替番号を割り当てるパーティションを割り当てます。
- d) ILS を通じてこの番号をアドバタイズする場合は、[ILS経由でグローバルにアドバタイズ (Advertise Globally via ILS)] チェックボックスをオンにします。アドバタイズされたパターンを使用して一定の代替番号の範囲を要約している場合は、個別の代替番号をアドバタイズする必要はありません。
- e) [PSTNフェールオーバー (PSTN Failover)] セクションを展開して、通常のコールルーティングが失敗した場合に使用する PSTN フェールオーバーとして、[エンタープライズ番号 (Enterprise Number)] または [+E.164代替番号 (+E.164 Alternate Number)] を選択します。

ステップ 5 [保存 (Save)] をクリックします。

次のタスク

[ユニバーサル デバイス テンプレートの設定 \(52 ページ\)](#)

ユニバーサル デバイス テンプレートの設定

ユニバーサル デバイス テンプレートを使用すると、新しくプロビジョニングしたデバイスに簡単に設定を適用できます。プロビジョニングされたデバイスは、ユニバーサル デバイス テンプレートの設定を使用します。さまざまなユーザグループのニーズを満たすために、異なるデバイステンプレートを設定できます。設定したプロファイルがこのテンプレートに割り当てることもできます。

始める前に

[ユニバーサル回線テンプレートの設定 \(51 ページ\)](#)

手順

-
- ステップ 1** Cisco Unified CM Administration で、[ユーザの管理 (User Management)] > [ユーザ/電話の追加 (User/Phone Add)] > [ユニバーサル デバイス テンプレート (Universal Device Template)] 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** 次の必須フィールドに入力します。
 - a) テンプレートの [デバイスの説明 (Device Description)] を入力します。
 - b) [デバイスプールタイプ (Device Pool Type)] を 65 Device Pools 選択します。
 - c) [デバイスのセキュリティプロファイル (Device Security Profile)] をドロップダウン リストから選択します。

- d) [SIPプロファイル (SIP Profile)] をドロップダウンリストから選択します。
- e) [電話ボタンテンプレート (Phone Button Template)] をドロップダウンリストから選択します。

ステップ 4 [ユニバーサルデバイステンプレートの設定 (Universal Device Template Configuration)] ウィンドウで、残りのフィールドを入力します。フィールドの説明については、オンラインヘルプを参照してください。

ステップ 5 [電話の設定 (Phone Settings)] で、次の任意指定のフィールドを入力します。

- a) [共通の電話プロファイル (Common Phone Profile)] を設定した場合は、そのプロファイルを割り当てます。
- b) [共通デバイス設定 (Common Device Configuration)] を設定した場合は、その設定を割り当てます。
- c) [機能管理ポリシー (Feature Control Policy)] を設定した場合は、そのポリシーを割り当てます。

ステップ 6 [保存 (Save)] をクリックします。

次のタスク

[ユーザ プロファイルの設定 \(53 ページ\)](#)

ユーザ プロファイルの設定

ユーザ プロファイルを使用して、ユニバーサル回線テンプレートとユニバーサル デバイス テンプレートをユーザに割り当てます。さまざまなユーザ グループ用に複数のユーザ プロファイルを設定します。このサービスプロファイルを使用するユーザに対してセルフプロビジョニングを有効にすることもできます。

始める前に

[ユニバーサル デバイス テンプレートの設定 \(52 ページ\)](#)

手順

-
- ステップ 1** [Cisco Unified CM 管理 (Cisco Unified CM Administration)] から、以下を選択します。[**ユーザ管理 (User Management)**] > [**ユーザ設定 (User Settings)**] > [**ユーザプロファイル (User Profile)**] 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** ユーザ プロファイルの [名前 (Name)] および [説明 (Description)] を入力します。
 - ステップ 4** [ユニバーサルデバイステンプレート (Universal Device Template)] を、ユーザの [デスクフォン (Desk Phones)]、[モバイルおよびデスクトップデバイス (Mobile and Desktop Devices)]、および [リモート接続先/デバイスプロファイル (Remote Destination/Device Profiles)] に割り当てます。

- ステップ 5** [ユニバーサル回線テンプレート (Universal Line Template)] をこのユーザ プロファイルのユーザの電話回線に適用するために割り当てます。
- ステップ 6** このユーザ プロファイルのユーザに自分の電話をプロビジョニングするセルフプロビジョニング機能の使用を許可するには、次の手順を実行します
- [エンドユーザに自分の電話のプロビジョニングを許可 (Allow End User to Provision their own phones)] チェックボックスをオンにします。
 - [エンドユーザーのプロビジョニングする電話数を制限 (Limit Provisioning once End User has this many phones)] フィールドに、ユーザーがプロビジョニングできる電話の最大数を入力します。最大値は 20 です。
 - このプロファイルに関連付けられたユーザーに、別のユーザーがすでに所有しているデバイスに移行または再割り当てする権限があるかどうかを判断するには、[すでに別のエンドユーザーに割り当てられた電話機のプロビジョニングを許可する (Allow Provisioning of a phone already assigned to a different End User)] 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 7** このユーザープロファイルに関連付けられた Cisco Jabber ユーザーがモバイルおよびリモートアクセス機能を使用できるようにするには、[モバイルおよびリモートアクセスの有効化 (Enable Mobile and Remote Access)] チェックボックスをオンにします。
- (注)
- デフォルトでは、このチェックボックスはオンです。このチェックボックスをオフにすると、[クライアントポリシー (Client Policies)] セクションが無効になり、サービスクライアント ポリシー オプションは、デフォルトで選択されません。
 - この設定は、OAuth 更新ログインを使用している Cisco Jabber のユーザにのみ必須です。非 Jabber ユーザは、この設定がなくてもモバイルおよびリモートアクセスを使用できます。モバイルおよびリモートアクセス機能は、Jabber のモバイルおよびリモートアクセスユーザにのみ適用され、他のエンドポイントまたはクライアントには適用されません。
- ステップ 8** このユーザ プロファイルに Jabber ポリシーを割り当てます。[デスクトップクライアントポリシー (Desktop Client Policy)] および [モバイルクライアントポリシー (Jabber Mobile Client Policy)] のドロップダウンリストから、次のいずれかのオプションを選択します。
- [サービスなし (No Service)] : このポリシーでは、すべての Cisco Jabber サービスへのアクセスが禁止されます。
 - [IM & Presence のみ (IM & Presence only)] : このポリシーは、インスタントメッセージとプレゼンス機能だけを有効にします。
 - [IM & Presence、音声およびビデオ通話 (IM & Presence, Voice and Video calls)] : このポリシーは、オーディオまたはビデオデバイスを所有しているすべてのユーザーに対して、インスタントメッセージング、プレゼンス、ボイスメール、および会議機能を有効にします。これがデフォルトのオプションです。

(注) Jabber デスクトップ クライアントには、Windows ユーザ用 Cisco Jabber と、Mac ユーザ用 Cisco Jabber が含まれています。Jabber モバイル クライアントには、iPad および iPhone ユーザ用 Cisco Jabber と、Android ユーザ用 Cisco Jabber が含まれています。

ステップ 9 このユーザ プロファイルのユーザが Cisco Unified Communications セルフケア ポータルで Extension Mobility または Extension Mobility Cross Cluster の最大ログイン時間を設定できるようにするには、[エンドユーザに Extension Mobility の最大ログイン時間の設定を許可する (Allow End User to set their Extension Mobility maximum login time)] チェックボックスをオンにします。

(注) デフォルトでは [エンド ユーザに Extension Mobility の最大ログイン時間の設定を許可する (Allow End User to set their Extension Mobility maximum login time)] チェック ボックスはオフになっています。

ステップ 10 [保存 (Save)] をクリックします。

次のタスク

[機能グループ テンプレートの設定 \(55 ページ\)](#)

機能グループ テンプレートの設定

機能グループテンプレートは、プロビジョニングされたユーザ用に、電話、回線、および機能をすばやく設定できるようにすることで、システムの展開をサポートします。企業の LDAP ディレクトリからユーザを同期している場合は、ディレクトリからユーザを同期させるユーザ プロファイルおよびサービス プロファイルを使用して機能グループ テンプレートを設定します。このテンプレートを使用して、同期されたユーザに対して IM and Presence Service を有効化することもできます。

手順

-
- ステップ 1** Cisco Unified CM Administration で、[ユーザ管理 (User Management)] > [ユーザ/電話の追加 (User/Phone Add)] > [機能グループ テンプレート (Feature Group Template)] を選択します。
 - ステップ 2** [新規追加 (Add New)] をクリックします。
 - ステップ 3** 機能グループ テンプレートの [名前 (Name)] と [説明 (Description)] を入力します。
 - ステップ 4** このテンプレートを使用するすべてのユーザのホーム クラスタとしてローカル クラスタを使用する場合は、[ホーム クラスタ (Home Cluster)] チェック ボックスをオンにします。
 - ステップ 5** このテンプレートを使用するユーザがインスタントメッセージおよびプレゼンス情報を交換できるようにするには、[Unified CM IM and Presenceのユーザを有効化 (Enable User for Unified CM IM and Presence)] チェックボックスをオンにします。

- ステップ 6** ドロップダウン リストから、[サービスプロファイル (Services Profile)] および [ユーザプロファイル (User Profile)] を選択します。
- ステップ 7** [機能グループ テンプレートの設定 (Feature Group Template Configuration)] ウィンドウの残りのフィールドに入力します。フィールドの説明については、オンラインヘルプを参照してください。
- ステップ 8** [保存 (Save)] をクリックします。

次のタスク

新規エンドユーザを追加します。システムが会社の LDAP ディレクトリと統合されている場合は、LDAP ディレクトリから直接ユーザをインポートできます。そうでない場合は、手動でエンドユーザを作成します。

- [LDAP からのエンドユーザのインポート \(56 ページ\)](#)
- [エンドユーザの手動追加 \(57 ページ\)](#)

LDAP からのエンドユーザのインポート

社内 LDAP ディレクトリから新しいエンドユーザを手動でインポートするには、次の手順に従います。LDAP 同期設定に、機能グループ テンプレートとユーザ プロファイル (ユニバーサル回線テンプレート、ユニバーサル デバイス テンプレートを含む) 、および DN プールが含まれている場合、インポート プロセスによりエンドユーザとプライマリ エクステンションが自動的に設定されます。



- (注) 初回同期の実行後には、新しい設定 (たとえば、機能グループ テンプレートの追加) を LDAP ディレクトリ同期に追加することはできません。既存の LDAP 同期を編集する場合は、一括管理を使用するか、または新しい LDAP 同期を設定する必要があります。

始める前に

この手順を開始する前に、Cisco Unified Communications Manager が社内の LDAP ディレクトリとすでに同期していることを確認します。LDAP 同期には、ユニバーサル回線テンプレートおよびユニバーサル デバイス テンプレートと機能グループ テンプレートが含まれている必要があります。

手順

- ステップ 1** Cisco Unified CM の管理で、[システム (System)] > [LDAP (LADP)] > [LDAP ディレクトリ (LDAP Directory)] を選択します。
- ステップ 2** [検索 (Find)] をクリックし、ユーザの追加先 LDAP ディレクトリを選択します。

ステップ3 [完全同期を実施 (Perform Full Sync)] をクリックします。

Cisco Unified Communications Manager が、外部の LDAP ディレクトリと同期します。LDAP ディレクトリ内の新しいエンドユーザが Cisco Unified Communications Manager データベースにインポートされます。

次のタスク

セルフプロビジョニングが有効になっている場合、エンドユーザがセルフプロビジョニング自動音声応答 (IVR) を使用して新しい電話機をプロビジョニングできます。有効になっていない場合は、次のタスクのいずれかを実行して、電話機をエンドユーザに割り当てます。

- [エンドユーザ用の新しい電話機の追加 \(58 ページ\)](#)
- [エンドユーザへの既存の電話機の移動 \(59 ページ\)](#)

エンドユーザの手動追加

次の手順を実行して、新しいエンドユーザを追加し、そのエンドユーザをアクセスコントロールグループとプライマリ回線内線番号を指定して設定します。



- (注) ユーザを割り当てる役割の権限を持つアクセス制御グループがすでに設定されていることを確認してください。詳細については、「ユーザアクセスの管理」の章を参照してください。

始める前に

ユニバーサル回線テンプレートを含むユーザプロファイルが設定されていることを確認します。新しい内線番号を設定する必要がある場合は、Cisco Unified Communications Manager でユニバーサル回線テンプレートの設定を使用してプライマリ内線番号を設定します。

手順

-
- ステップ1** Cisco Unified CM の管理で、[ユーザ管理 (User Management)] > [ユーザ/電話の追加 (User/Phone Add)] > [ユーザ/電話のクイック追加 (Quick User/Phone Add)] を選択します。
 - ステップ2** ユーザの [ユーザ ID (User ID)] と [姓 (Last Name)] を入力します。
 - 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で、機能グループテンプレートを選択します。
 - ステップ4** [保存 (Save)] をクリックします。
 - ステップ5** [ユーザプロファイル (User Profile)] ドロップダウンリストで、選択したユーザプロファイルにユニバーサル回線テンプレートが含まれていることを確認します。
 - ステップ6** [アクセスコントロールグループメンバーシップ (Access Control Group Membership)] セクションで、[+] アイコンをクリックします。

- ステップ 7** [ユーザの所属グループ (User is a member of)] ドロップダウンリストで、アクセスコントロールグループを選択します。
- ステップ 8** [プライマリ内線番号 (Primary Extension)] の下で、[+] アイコンをクリックします。
- ステップ 9** [内線番号 (Extension)] ドロップダウンリストで、[(使用可能) (available)] として表示されている DN を選択します。
- ステップ 10** すべての回線内線番号が [(使用済み) (used)] と表示されている場合は、次の手順を実行します。
- [新規... (New...)] ボタンをクリックします。
[新規内線の追加 (Add New Extension)] ポップアップが表示されます。
 - [電話番号 (Directory Number)] フィールドに、新しい回線内線番号を入力します。
 - [回線テンプレート (Line Template)] ドロップダウンリストから、ユニバーサル回線テンプレートを選択します。
 - [OK] をクリックします。
Cisco Unified Communications Manager が、ユニバーサル回線テンプレートの設定を使用して電話番号を設定します。
- ステップ 11** (任意) [ユーザ/電話のクイック追加設定 (Quick User/Phone Add Configuration)] ウィンドウで、追加のフィールドに値を入力します。
- ステップ 12** [保存 (Save)] をクリックします。

次のタスク

次の手順のいずれかを実行して、このエンドユーザに電話機を割り当てます。

- [エンドユーザ用の新しい電話機の追加 \(58 ページ\)](#)
- [エンドユーザへの既存の電話機の移動 \(59 ページ\)](#)

エンドユーザ用の新しい電話機の追加

次の手順を実行して、新しいエンドユーザまたは既存のエンドユーザ用の新しい電話機を追加します。エンドユーザのユーザプロファイルにユニバーサルデバイステンプレートが含まれていることを確認します。Cisco Unified Communications Manager が、ユニバーサルデバイステンプレートの設定を使用して電話機を設定します。

始める前に

次の手順のいずれかを実行して、エンドユーザを追加します。

- [エンドユーザの手動追加 \(57 ページ\)](#)
- [LDAP からのエンドユーザのインポート \(56 ページ\)](#)

手順

-
- ステップ 1 Cisco Unified CM Administration で、[ユーザ管理 (User Management)] > [ユーザ/電話の追加 (User/Phone Add)] > [ユーザ/電話のクイック追加 (Quick User/Phone Add)] を選択します。
 - ステップ 2 [検索 (Find)] をクリックして、新しい電話機を追加するユーザを選択します。
 - ステップ 3 [デバイスの管理 (Manage Devices)] ボタンをクリックします。
[デバイスの管理 (Manage Devices)] ウィンドウが表示されます。
 - ステップ 4 [電話の新規追加 (Add New Phone)] をクリックします。
[ユーザに電話を追加 (Add Phone to User)] ポップアップが表示されます。
 - ステップ 5 [製品タイプ (Product Type)] ドロップダウンリストで、電話機モデルを選択します。
 - ステップ 6 [デバイス プロトコル (Device Protocol)] ドロップダウンリストから、プロトコルとして [SIP] または [SCCP] を選択します。
 - ステップ 7 [デバイス名 (Device Name)] テキストボックスに、デバイスの MAC アドレスを入力します。
 - ステップ 8 [ユニバーサルデバイス テンプレート (Universal Device Template)] ドロップダウンリストで、ユニバーサル デバイス テンプレートを選択します。
 - ステップ 9 電話機が拡張モジュールをサポートしている場合は、展開する拡張モジュールの数を入力します。
 - ステップ 10 Extension Mobility を使用して電話機にアクセスするには、[Extension Mobility 内 (In Extension Mobility)] チェック ボックスをオンにします。
 - ステップ 11 [電話の追加 (Add Phone)] をクリックします。
[電話の新規追加 (Add New Phone)] ポップアップが閉じます。Cisco Unified Communications Manager が、電話機をユーザに追加し、ユニバーサルデバイス テンプレートを使用してその電話機を設定します。
 - ステップ 12 電話機の設定に追加の編集を加えるには、対応する鉛筆アイコンをクリックして、[電話の設定 (Phone Configuration)] ウィンドウで電話機を開きます。
-

エンドユーザへの既存の電話機の移動

次の手順を実行して、既存の電話機を新しいまたは既存のエンドユーザに移動します。

手順

-
- ステップ 1 Cisco Unified CM の管理で、[ユーザ管理 (User Management)] > [ユーザ/電話の追加 (User/Phone Add)] > [ユーザ/電話のクイック追加 (Quick User/Phone Add)] を選択します。
 - ステップ 2 [検索 (Find)] をクリックして、既存の電話機を移動するユーザを選択します。
 - ステップ 3 [デバイスの管理 (Manage Devices)] ボタンをクリックします。
 - ステップ 4 [このユーザに移動する電話の検索 (Find a Phone to Move To This User)] ボタンをクリックします。

ステップ5 このユーザに移動する電話機を選択します。

ステップ6 [選択項目の移動 (Move Selected)] をクリックします。

エンドユーザ PIN の変更

手順

- ステップ1 Cisco Unified Communications Manager Administration で、[ユーザ管理 (User Management)] > [エンドユーザ (End User)] を選択します。
[ユーザの検索と一覧表示 (Find and List Users)] ウィンドウが表示されます。
- ステップ2 既存のユーザを選択するには、[ユーザを次の条件で検索 (Find User where)] フィールドで適切なフィルタを指定し、[検索 (Find)] をクリックしてユーザのリストを取得した後、リストからユーザを選択します。
[エンドユーザ設定 (End User Configuration)] ウィンドウが表示されます。
- ステップ3 [PIN] フィールドで、暗号化された既存の PIN をダブルクリックして、新しい PIN を入力します。割り当てられている資格情報ポリシーに指定されている文字数以上 (1 ~ 127 文字) を入力する必要があります。
- ステップ4 [PIN の確認 (Confirm PIN)] フィールドで、既存の暗号化された PIN をダブルクリックし、もう一度、新しい PIN を入力します。
- ステップ5 [保存 (Save)] をクリックします。

(注) Cisco Unity Connection の [アプリケーション サーバの設定 (Application Server Configuration)] ウィンドウで [エンドユーザ PIN の同期 (End User Pin synchronization)] チェックボックスが有効になっている場合は、エクステンション モビリティ、開催中の会議、モバイル コネクト、および Cisco Unity Connection ボイスメールに同じエンドユーザ PIN を使用してログインできます。エンドユーザは、同じ PIN を使用して、エクステンション モビリティにログインし、自分のボイスメールにアクセスできます。

エンドユーザ パスワードの変更

LDAP 認証が有効になっている場合は、エンドユーザ パスワードを変更できません。

手順

- ステップ1 Cisco Unified Communications Manager Administration で、[ユーザ管理 (User Management)] > [エンドユーザ (End User)] を選択します。
[ユーザの検索と一覧表示 (Find and List Users)] ウィンドウが表示されます。

- ステップ 2** 既存のユーザを選択するには、[ユーザを次の条件で検索 (Find User where)] フィールドで適切なフィルタを指定し、[検索 (Find)] をクリックしてユーザのリストを取得した後、リストからユーザを選択します。
[エンドユーザ設定 (End User Configuration)] ウィンドウが表示されます。
- ステップ 3** [パスワード (Password)] フィールドで、暗号化された既存のパスワードをダブルクリックして、新しいパスワードを入力します。割り当てられている資格情報ポリシーに指定されている文字数以上 (1 ~ 127 文字) を入力する必要があります。
- ステップ 4** [パスワードの確認 (Confirm Password)] フィールドで、既存の暗号化されたパスワードをダブルクリックし、もう一度、新しいパスワードを入力します。
- ステップ 5** [保存 (Save)] をクリックします。

Cisco Unity Connection ボイス メールボックスの作成

始める前に

- Cisco Unified Communications Manager をボイス メッセージング用に設定する必要があります。Cisco Unity Connection を使用するように Cisco Unified Communications Manager を設定する方法については、次で『*System Configuration Guide for Cisco Unified Communications Manager*』を参照してください。

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

- デバイスとプライマリ内線番号をエンドユーザに関連付ける必要があります。
- このセクションで説明する手順を実行する代わりに、Cisco Unity Connection で使用可能なインポート機能を使用できます。インポート機能の使用方法については、『*User Moves, Adds, and Changes Guide for Cisco Unity Connection*』を参照してください

手順

- ステップ 1** Cisco Unified Communications Manager Administration で、[ユーザ管理 (User Management)] > [エンドユーザ (End User)] を選択します。
[ユーザの検索と一覧表示 (Find and List Users)] ウィンドウが表示されます。
- ステップ 2** 既存のユーザを選択するには、[ユーザを次の条件で検索 (Find User where)] フィールドで適切なフィルタを指定し、[検索 (Find)] をクリックしてユーザのリストを取得した後、リストからユーザを選択します。
[エンドユーザ設定 (End User Configuration)] ウィンドウが表示されます。
- ステップ 3** プライマリ内線番号がこのユーザに関連付けられていることを確認します。
- (注) プライマリ内線番号を定義する必要があります。そうしなかった場合は、[関連リンク (Related Links)] ドロップダウンリストに Cisco Unity ユーザリンクが表示されません。

ステップ 4 [関連リンク (Related Links)] ドロップダウンリストで、[Cisco Unity ユーザの作成 (Create Cisco Unity User)] リンクを選択してから、[移動 (Go)] をクリックします。

[Cisco Unity ユーザの追加 (Add Cisco Unity User)] ダイアログボックスが表示されます。

ステップ 5 [アプリケーションサーバ (Application Server)] ドロップダウンリストで、Cisco Unity Connection ユーザを作成する Cisco Unity Connection サーバを選択してから、[次へ (Next)] をクリックします。

ステップ 6 [サブスクリイバテンプレート (Subscriber Template)] ドロップダウンリストで、使用するサブスクリイバテンプレートを選択します。

ステップ 7 [保存 (Save)] をクリックします。

メールボックスが作成されます。[エンドユーザの設定 (End User Configuration)] ウィンドウの [関連リンク (Related Links)] ドロップダウンリスト内のリンクが [Cisco Unity ユーザの編集 (Edit Cisco Unity User)] に変化します。これで、Cisco Unity Connection Administration で、作成したユーザを確認できます。

(注) Cisco Unity Connection ユーザと Cisco Unified Communications Manager エンドユーザを統合した後は、[エイリアス (Alias)] (Cisco Unified CM の管理内のユーザ ID)、[名 (First Name)]、[姓 (Last Name)]、[内線番号 (Extension)] (Cisco Unified CM の管理内のプライマリ内線番号) などの Cisco Unified CM の管理内のフィールドを編集できなくなります。これらのフィールドは、Cisco Unified CM の管理でしか更新できません。



第 6 章

アプリケーションユーザの管理

- [アプリケーションユーザの概要 \(63 ページ\)](#)
- [アプリケーションユーザのタスクフロー \(64 ページ\)](#)

アプリケーションユーザの概要

Cisco Unified CM の管理の [アプリケーションユーザの設定 (Application User Configuration)] ウィンドウで管理者は、Unified Communications Manager アプリケーションユーザに関する情報を追加、検索、表示、および保守することができます。

Cisco Unified CM の管理には、デフォルトで以下のアプリケーションユーザが設定されています。

- CCMAAdministrator
- CCMSysUser
- CCMQRTSecureSysUser
- CCMQRTSysUser
- IPMASecureSysUser
- IPMASysUser
- WDSecureSysUser
- WDSysUser
- TabSyncSysUser
- CUCService



(注) Standard CCM Super Users グループの管理者ユーザは、Cisco Unified Communications Manager Administration、Cisco Unified Serviceability、および Cisco Unified Reporting のいずれかにシングルサインオンすることによって、このすべてのアプリケーションにアクセスできます。

アプリケーションユーザのタスクフロー

手順

	コマンドまたはアクション	目的
ステップ 1	新規アプリケーションユーザの追加 (64 ページ)	新しいアプリケーションユーザを追加します。
ステップ 2	デバイスとアプリケーションユーザの関連付け (65 ページ)	アプリケーションユーザに関連付けるデバイスを割り当てます。
ステップ 3	Cisco Unity または Cisco Unity Connection への管理者ユーザの追加 (65 ページ)	Cisco Unity または Cisco Unity Connection に管理者ユーザとしてユーザを追加します。Cisco Unified CM の管理でアプリケーションユーザを設定します。その後で、Cisco Unity または Cisco Unity Connection で、そのユーザの追加の設定を構成します。
ステップ 4	アプリケーションユーザパスワードの変更 (67 ページ)	アプリケーションユーザパスワードを変更します。
ステップ 5	アプリケーションユーザパスワードクレデンシャル情報の管理 (67 ページ)	関連する認証ルール、関連するクレデンシャルポリシー、アプリケーションユーザの直前のパスワード変更の時刻などのクレデンシャル情報を変更または表示します。

新規アプリケーションユーザの追加

手順

-
- ステップ 1 Cisco Unified CM の管理で、[ユーザの管理 (User Management)] > [アプリケーションユーザ (Application User)] 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 [アプリケーションユーザの設定 (Application User Configuration)] ウィンドウのフィールドを設定します。フィールドとその設定オプションの詳細については、オンラインヘルプを参照してください。
- ステップ 4 [保存 (Save)] をクリックします。
-

次のタスク

[デバイスとアプリケーションユーザの関連付け \(65 ページ\)](#)

デバイスとアプリケーションユーザの関連付け

手順

-
- ステップ 1** Cisco Unified CM Administration から、[ユーザの管理 (User Management)] > [アプリケーションユーザ (Application User)] を選択します。
[ユーザの検索と一覧表示 (Find and List Users)] ウィンドウが表示されます。
- ステップ 2** 既存のユーザを選択するには、[次の条件でユーザを検索 (Find User Where)] フィールドに適切なフィルタを指定し、[検索 (Find)] を選択してユーザのリストを取得し、リストからユーザを選択します。
- ステップ 3** [使用可能なデバイス (Available Devices)] リストで、アプリケーションユーザに関連付けするデバイスを選択し、リストの下にある下向き矢印をクリックします。選択したデバイスが [制御対象のデバイス (Controlled Devices)] リストに移動します。
- (注) 使用可能なデバイスのリストを制限するには、[別の電話を検索 (Find more Phones)] ボタンまたは [別のルートポイントを検索 (Find more Route Points)] ボタンをクリックします。
- ステップ 4** [別の電話を検索 (Find more Phones)] ボタンをクリックすると、[電話の検索/一覧表示 (Find and List Phones)] ウィンドウが表示されます。検索を実行して、このアプリケーションユーザに関連付ける電話機を検索します。
- アプリケーションユーザに割り当てるデバイスごとに、上記ステップを繰り返します。
- ステップ 5** [別のルートポイントを検索 (Find more Route Points)] ボタンをクリックすると、[CTI ルートポイントの検索/一覧表示 (Find and List CTI Route Points)] ウィンドウが表示されます。検索を実行して、このアプリケーションユーザに関連付ける CTI ルートポイントを検索します。
- アプリケーションユーザに割り当てるデバイスごとに、上記ステップを繰り返します。
- ステップ 6** [保存 (Save)] をクリックします。
-

Cisco Unity または Cisco Unity Connection への管理者ユーザの追加

Cisco Unified Communications Manager と Cisco Unity Connection 7.x 以降を統合する場合は、このセクションで説明する手順を実行する代わりに、Cisco Unity Connection 7.x 以降で使用可能なインポート機能を使用できます。インポート機能の使用方法については、次で Cisco Unity Connection 7.x 以降の『*User Moves, Adds, and Changes Guide*』を参照してください。

<http://www.cisco.com/c/en/us/support/unified-communications/unity-connection/products-maintenance-guides-list.html>。

Cisco Unity または Cisco Unity Connection ユーザが Cisco Unified CM アプリケーション ユーザと統合されている場合は、フィールドを編集できません。これらのフィールドは、Cisco Unified Communications Manager Administration でしか更新できません。

Cisco Unity と Cisco Unity Connection は、Cisco Unified Communications Manager からのデータの同期をモニタします。ツールメニューの [Cisco Unity Administration] または [Cisco Unity Connection Administration] で同期時刻を設定できます。

始める前に

Cisco Unity または Cisco Unity Connection にプッシュする予定のユーザに適切なテンプレートが定義されていることを確認します

[Cisco Unity ユーザの作成 (Create Cisco Unity User)] リンクは、適切な Cisco Unity または Cisco Unity Connection ソフトウェアがインストールされ、設定されている場合にのみ表示されます。Cisco Unity に関する『*Cisco Unified Communications Manager Integration Guide*』または Cisco Unity Connection に関する『*Cisco Unified Communications Manager SCCP Integration Guide*』を次で参照してください。

<http://www.cisco.com/c/en/us/support/unified-communications/unity-connection/products-installation-and-configuration-guides-list.html>。

手順

-
- ステップ 1 Cisco Unified CM の管理から、[ユーザ管理 (User Management)] > [アプリケーション ユーザ (Application User)] を選択します。
 - ステップ 2 既存のユーザを選択するには、[次の条件でユーザを検索 (Find User Where)] フィールドに適切なフィルタを指定し、[検索 (Find)] を選択してユーザのリストを取得し、リストからユーザを選択します。
 - ステップ 3 [関連リンク (Related Links)] ドロップダウンリストで、[Cisco Unity アプリケーション ユーザの作成 (Create Cisco Unity Application User)] リンクを選択し、[移動 (Go)] をクリックします。
[Cisco Unity ユーザの追加 (Add Cisco Unity User)] ダイアログが表示されます。
 - ステップ 4 [アプリケーション サーバ (Application Server)] ドロップダウンリストで、Cisco Unity または Cisco Unity Connection ユーザを作成する Cisco Unity または Cisco Unity Connection サーバを選択し、[次へ (Next)] をクリックします。
 - ステップ 5 [アプリケーション ユーザ テンプレート (Application User Template)] ドロップダウンリストで、使用するテンプレートを選択します。
 - ステップ 6 [保存 (Save)] をクリックします。
Cisco Unity または Cisco Unity Connection で管理者アカウントが作成されます。[アプリケーション ユーザの設定 (Application User Configuration)] ウィンドウの [関連リンク (Related Links)] 内のリンクが [Cisco Unity ユーザの編集 (Edit Cisco Unity User)] に変化します。これで、Cisco Unity Administration または Cisco Unity Connection Administration で作成したユーザを表示できるようになります。
-

アプリケーションユーザパスワードの変更

手順

- ステップ 1 Cisco Unified CM Administration から、[ユーザの管理 (User Management)] > [アプリケーションユーザ (Application User)] を選択します。
[ユーザの検索と一覧表示 (Find and List Users)] ウィンドウが表示されます。
- ステップ 2 既存のユーザを選択するには、[次の条件でユーザを検索 (Find User Where)] フィールドに適切なフィルタを指定し、[検索 (Find)] を選択してユーザのリストを取得し、リストからユーザを選択します。
[アプリケーションユーザの設定 (Application User Configuration)] ウィンドウに、選択されたアプリケーションユーザに関する情報が表示されます。
- ステップ 3 [パスワード (Password)] フィールドで、既存の暗号化されたパスワードをダブルクリックし、新しいパスワードを入力します。
- ステップ 4 [パスワードの確認 (Confirm Password)] フィールドで、既存の暗号化されたパスワードをダブルクリックし、もう一度、新しいパスワードを入力します。
- ステップ 5 [保存 (Save)] をクリックします。

アプリケーションユーザパスワードクレデンシャル情報の管理

次の手順を実行して、アプリケーションユーザパスワードに関するクレデンシャル情報を管理します。これにより、パスワードのロック、パスワードへのクレデンシャルポリシーの適用、最後に失敗したログイン試行時などの情報の表示などの管理業務を実行できます。

手順

- ステップ 1 Cisco Unified CM Administration から、[ユーザの管理 (User Management)] > [アプリケーションユーザ (Application User)] を選択します。
[ユーザの検索と一覧表示 (Find and List Users)] ウィンドウが表示されます。
- ステップ 2 既存のユーザを選択するには、[次の条件でユーザを検索 (Find User Where)] フィールドに適切なフィルタを指定し、[検索 (Find)] を選択してユーザのリストを取得し、リストからユーザを選択します。
[アプリケーションユーザの設定 (Application User Configuration)] ウィンドウに、選択されたアプリケーションユーザに関する情報が表示されます。
- ステップ 3 パスワード情報を変更または表示するには、[パスワード (Password)] フィールドの横にある [クレデンシャルの編集 (Edit Credential)] ボタンをクリックします。
ユーザの [クレデンシャル設定 (Credential Configuration)] が表示されます。
- ステップ 4 [クレデンシャル設定 (Credential Configuration)] ウィンドウで、各フィールドを設定します。
フィールドとその設定オプションの詳細については、オンラインヘルプを参照してください。

ステップ 5 いずれかの設定を変更した場合は、[保存 (Save)]をクリックします。



第 III 部

デバイスの管理

- [電話の管理 \(71 ページ\)](#)
- [デバイス ファームウェアの管理 \(93 ページ\)](#)
- [インフラストラクチャ デバイスの管理 \(101 ページ\)](#)



第 7 章

電話の管理

- [電話管理の概要 \(71 ページ\)](#)
- [電話ボタンテンプレート \(71 ページ\)](#)
- [電話機管理タスク \(72 ページ\)](#)

電話管理の概要

この章では、ネットワーク内の電話を管理する方法について説明します。このトピックでは、新しい電話の追加、既存の電話の別のユーザへの移動、電話のロック、電話のリセットなどのタスクについて説明します。

ご使用の電話機モデルの『Cisco IP Phone Administration Guide』には、該当する電話機モデルに固有の設定情報が記載されています。

電話ボタンテンプレート

電話ボタンテンプレートは、電話機モデルに基づいて作成されます。一部の電話機モデルでは、特定の電話ボタンテンプレートを使用しませんが、一部電話機モデルには、個々のテンプレートまたはデバイスのデフォルトテンプレートのいずれかの特定されたテンプレートが必要です。

[エンタープライズパラメータの設定 (Enterprise Parameters Configuration)] ページの [非サイズセーフ電話機の電話テンプレートの選択 (Phone Template Selection for Non-Size Safe Phone)] と [自動登録レガシーモード (Auto Registration Legacy Mode)] エンタープライズパラメータは、使用される電話ボタンテンプレートのタイプを指定します。フィールドの詳細については、オンラインヘルプを参照してください。

表 4: さまざまなシナリオにおける電話ボタン テンプレート

非サイズ セーフ電話機の電話テンプレートの選択	自動登録レガシー モード	電話
個々のテンプレートの作成	False	ユニバーサルデバイステンプレートからの電話を追加するときに、個々の電話ボタンテンプレートが作成されます。
デバイスのデフォルトからのテンプレートの使用	False	個々の電話ボタンテンプレートは作成されず、デバイスのデフォルトからの電話ボタンテンプレートを取得します。
デバイスのデフォルトからのテンプレートの使用	True	デバイス プール、電話テンプレート、コーリングサーチスペース、電話ボタンテンプレートの値は、デバイスのデフォルトから取得されます。
個々のテンプレートの作成	True	デバイス プール、電話テンプレート、コーリングサーチスペース、電話ボタンテンプレートの値は、デバイスのデフォルトから取得されます。 個々のテンプレートは作成されません。 自動登録レガシー モードには、優先度があります。

電話機管理タスク

手順

	コマンドまたはアクション	目的
ステップ 1	エンドユーザの有無にかかわらず新しい電話機の追加 (74 ページ)	エンドユーザの有無にかかわらずユニバーサルデバイステンプレートからの新しい電話機の追加
ステップ 2	電話機の手動での追加 (73 ページ)	デバイステンプレートなしでのエンドユーザの新しい電話機の追加

	コマンドまたはアクション	目的
ステップ 3	エンドユーザがあるテンプレートからの新しい電話機の追加 (76 ページ)	エンドユーザ用の新しい電話機を追加して、ユニバーサル デバイス テンプレートを割り当てます。
ステップ 4	既存の電話機の移動 (85 ページ)	設定された電話機を別のエンドユーザに移動します。
ステップ 5	現在ログイン中のデバイスの検索 (86 ページ)	特定のデバイスを検索するか、ユーザが現在ログインしているすべてのデバイスを列挙します。
ステップ 6	リモート ログイン デバイスの検索 (87 ページ)	特定のデバイスを検索するか、ユーザがリモートでログインしているすべてのデバイスを列挙します。
ステップ 7	電話機のリモート ロック (88 ページ)	一部の電話機は、リモートでロックすることができます。電話機をリモートでロックすると、ロックを解除するまで使用できなくなります。
ステップ 8	工場出荷時の初期状態への電話機のリセット (88 ページ)	電話機を工場出荷時の設定にリセットします。
ステップ 9	電話ロック/ワイプレポート (89 ページ)	リモートでロックされたデバイスまたはリモートでファクトリーデフォルト設定にリセットされたデバイスを検索します。
ステップ 10	電話の LSC ステータスの表示および CAPF レポートの生成 (90 ページ)	電話機で LSC 失効ステータスを検索し、CAPF レポートも生成します。

電話機の手動での追加

次の手順を実行して、ユーザ用の新しい電話機を手動で追加します。

手順

- ステップ 1 [Cisco Unified CM の管理 (Cisco Unified CM Administration)] から、[デバイス (Device)] > [電話 (Phone)] > [電話の検索とリスト (Find and List Phones)] の順に選択します。
- ステップ 2 [電話の検索とリスト (Find and List Phones)] ページから [新規追加 (Add New)] をクリックして電話機を手動で追加します。
[新しい電話の追加 (Add a New Phone)] ページが表示されます。

[新しい電話の追加 (Add a New Phone)] ページから、[「ここをクリックしてユニバーサルデバイス テンプレートを追加 (click here to add a new phone using a Universal Device Template) 」] ハイパーリンクをクリックすると、ページは [新しい電話の追加 (Add a New Phone)] ページにリダイレクトされ、ユーザの追加の有無にかかわらずテンプレートから電話を追加します。詳細については、[エンドユーザの有無にかかわらずテンプレートからの新しい電話機の追加 \(74 ページ\)](#) を参照してください。

ステップ 3 [電話のタイプ (Phone Type)] ドロップダウンリストから、電話機モデルを選択します。

ステップ 4 [次へ (Next)] をクリックします。

[電話機の設定 (Phone Configuration)] ページが表示されます。

ステップ 5 [電話機の設定 (Phone Configuration)] ページで、必須フィールドに値を入力します。フィールドの詳細については、オンライン ヘルプを参照してください。

[製品固有の設定 (Product Specific Configuration)] 領域のフィールドの詳細については、ご使用の電話機モデルの『*Cisco IP Phone Administration Guide*』を参照してください。

ステップ 6 電話の設定を保存する場合は、[保存 (Save)] をクリックします。

次のタスク

[エンドユーザへの既存の電話機の移動 \(59 ページ\)](#)

エンドユーザの有無にかかわらずテンプレートからの新しい電話機の追加

次の手順を実行して、ユーザを追加するかどうかにかかわらず、テンプレートから新しい電話機を追加します。Cisco Unified Communications Manager が、ユニバーサルデバイス テンプレートの設定を使用して電話機を設定します。

始める前に

Cisco Unified Communications Manager でユニバーサルデバイス テンプレートが設定済みであることを確認します。

手順

ステップ 1 [Cisco Unified CM の管理 (Cisco Unified CM Administration)] から、[デバイス (Device)] > [電話 (Phone)] > [電話の検索とリスト (Find and List Phones)] の順に選択します。

ステップ 2 [電話の検索とリスト (Find and List Phones)] ページから、[テンプレートからの新規の追加 (Add New From Template)] をクリックして、エンドユーザの追加にかかわらずデバイス テンプレートからの電話を追加します。

[新しい電話の追加 (Add a New Phone)] ページが表示されます。

[新しい電話の追加 (Add a New Phone)] ページから、[「ここをクリックしてすべての電話設定を手動で入力する (click here to enter all phone settings manually)」] ハイパーリンクをクリックすると、ページは電話を手動で追加できる既存の [新しい電話の追加 (Add a New Phone)] ページにリダイレクトされます。詳細については、[電話機の手動での追加 \(73 ページ\)](#) を参照してください。

ステップ 3 [製品タイプ (およびプロトコル) (Phone Type (and Protocol))] ドロップダウンリストで、電話機モデルを選択します。

プロトコルのドロップダウンリストは、電話が複数のプロトコルをサポートしている場合にのみ表示されます。

ステップ 4 [名前または MAC アドレス (Name or MAC Address)] テキストボックスに、名前または MAC アドレスを入力します。

ステップ 5 [デバイステンプレート (Device Template)] ドロップダウンリストで、ユニバーサル デバイス テンプレートを選択します。

ステップ 6 [電話番号 (回線 1) (Directory Number (Line 1))] ドロップダウンリストで、電話番号を選択します。

ドロップダウンリストのディレクトリ番号がドロップダウンリストの上限を越えている場合、[検索 (Find)] タブが表示されます。[検索 (Find)] をクリックすると、ディレクトリ番号の検索条件を示すポップアップ ダイアログボックスが開きます。

ステップ 7 (オプション) 新しいディレクトリ番号を作成してデバイスに割り当てる場合には、[新規 (New)] をクリックしてディレクトリ番号を入力し、ユニバーサル回線テンプレートを選択します。

[ユーザ管理 (User Management)] > [ユーザ/電話の追加 (User/Phone Add)] > [ユーザ/電話のクイック追加 (Quick/User Phone Add)] に移動して、ユーザに関連付けられたディレクトリ番号を使用して電話を作成することもできます。

ステップ 8 (オプション) [ユーザ (User)] ドロップダウンリストから、新しい電話機を追加するエンドユーザを選択します。

(注) Cisco デュアル モード (モバイル) デバイスのユーザを選択する場合には必須です。

ドロップダウンリストのエンドユーザの数がドロップダウンリストの上限を越えている場合、[検索 (Find)] タブが表示されます。[検索 (Find)] をクリックすると、エンドユーザ検索条件を示すポップアップ ダイアログボックスが開きます。

ステップ 9 [Add] をクリックします。

(注) 非サイズセーフ電話機の場合、電話テンプレートは [エンタープライズパラメータの設定 (Enterprise Parameters Configuration)] ページの [非サイズセーフ電話機の電話テンプレートの選択 (Phone Template Selection for Non-Size Safe Phone)] と [自動登録レガシーモード (Auto Registration Legacy Mode)] パラメータの選択に基づいて作成されます。

追加が成功したとのメッセージが表示されます。Cisco Unified Communications Manager で電話機が追加され、[電話の設定 (Phone Configuration)] ページが表示されます。[電話の設定 (Phone

Configuration)] ページのフィールドの詳細については、オンラインヘルプを参照してください。

次のタスク

[エンドユーザへの既存の電話機の移動 \(59 ページ\)](#)

エンドユーザがあるテンプレートからの新しい電話機の追加

次の手順を実行して、エンドユーザ用の新しい電話機を追加します。

始める前に

電話機追加対象のエンドユーザは、ユニバーサルデバイステンプレートを含むユーザプロフィールがセットアップされています。Cisco Unified Communications Manager が、ユニバーサルデバイステンプレートの設定を使用して電話機を設定します。

- [エンドユーザ管理タスク \(49 ページ\)](#)

手順

- ステップ 1 Cisco Unified CM Administration で、[ユーザ管理 (User Management)] > [ユーザ/電話の追加 (User/Phone Add)] > [ユーザ/電話のクイック追加 (Quick User/Phone Add)] を選択します。
- ステップ 2 [検索 (Find)] をクリックして、新しい電話機を追加するユーザを選択します。
- ステップ 3 [デバイスの管理 (Manage Devices)] ボタンをクリックします。
[デバイスの管理 (Manage Devices)] ウィンドウが表示されます。
- ステップ 4 [電話の新規追加 (Add New Phone)] をクリックします。
[ユーザに電話を追加 (Add Phone to User)] ポップアップが表示されます。
- ステップ 5 [製品タイプ (Product Type)] ドロップダウンリストで、電話機モデルを選択します。
- ステップ 6 [デバイスプロトコル (Device Protocol)] ドロップダウンリストから、プロトコルとして [SIP] または [SCCP] を選択します。
- ステップ 7 [デバイス名 (DeviceName)] テキストボックスに、デバイスの MAC アドレスを入力します。
- ステップ 8 [ユニバーサルデバイステンプレート (Universal Device Template)] ドロップダウンリストで、ユニバーサルデバイステンプレートを選択します。
- ステップ 9 電話機が拡張モジュールをサポートしている場合は、展開する拡張モジュールの数を入力します。
- ステップ 10 Extension Mobility を使用して電話機にアクセスするには、[Extension Mobility 内 (In Extension Mobility)] チェックボックスをオンにします。
- ステップ 11 [電話の追加 (Add Phone)] をクリックします。

[電話の新規追加 (Add New Phone)] ポップアップが閉じます。Cisco Unified Communications Manager が、電話機をユーザに追加し、ユニバーサル デバイス テンプレートを使用してその電話機を設定します。

ステップ 12 電話機の設定に追加の編集を加えるには、対応する鉛筆アイコンをクリックして、[電話の設定 (Phone Configuration)] ウィンドウで電話機を開きます。

コラボレーション モバイル コンバージェンス 仮想デバイスの概要

CMC デバイスは、それに関連付けられたリモート接続先を表す仮想デバイスです。エンタープライズ電話で CMC デバイスにコールすると、コールはリモート接続先にリダイレクトされます。この機能は、デバイス タイプ [Collaboration モバイル コンバージェンス (Collaboration Mobile Convergence)] を作成することを目的としています。このデバイス タイプはいくつかのカスタマイズがされた Spark リモート デバイスと同じであり、以下の利点を提供します。

- Spark リモート デバイスと同様の機能を持つネイティブ モバイル デバイスを Cisco Unified Communications Manager 上でサポートします。
- 将来の開発機能パリティを含む機能を持つ Spark-RD として利用します。
- モバイルからデスクフォン、デスクフォンからモバイルへコールの移動などの、モバイル固有のユース ケースのカスタマイズができます。(ID ページで deskpickup タイマーを追加し、製品サポート機能の設定で有効にします)。
- CMC デバイスは、ハント グループに含めることができます。
- Spark リモート デバイスで共有回線に対応できます。
- ライセンス：ライセンス使用パースペクティブに応じて個別のデバイスとしてカウントします。複数デバイス ライセンス バンドルはいずれも、CMC RD をサポートする必要があります。

CMC RD デバイス ライセンスの調整

新しい CMC デバイスは、追加されると、ユーザに関連付けられているデバイスの数/タイプに基づいてライセンスを使用します。CMC デバイスによって使用されるライセンスのタイプは、それに関連付けられているエンド ユーザが所有するデバイスの数によって異なります。

- CMC デバイスのみを導入する場合は、拡張ライセンスを使用します。
- CMC デバイスと Spark RD を導入する場合は、拡張ライセンスを使用します。
- CMC と物理デバイス：拡張 Plus ライセンス
- CMC、Spark RD、および物理デバイスの場合：拡張 Plus ライセンス

Collaboration モバイル コンバージェンスの仮想デバイスを追加します。

エンド ユーザ用に Cisco Collaboration モバイル コンバージェンス (CMC) リモート デバイスを追加する次の手順を実行します。

始める前に

電話機追加対象のエンド ユーザは、ユニバーサル デバイス テンプレートを含むユーザ プロファイルがセットアップされている必要があります。Cisco Unified Communications Manager が、ユニバーサル デバイス テンプレートの設定を使用して電話機を設定します。

手順

- ステップ 1 Cisco Unified CM Administration で、[デバイス (Device)] > [電話 (Phone)] を選択します。
- ステップ 2 [新規追加 (Add New)] ボタンをクリックします。
- ステップ 3 [ここをクリックしてすべての電話設定を手動で入力する (Click here to enter all phone settings manually)] リンクをクリックします。
[新規電話を追加 (Add a New Phone)] ウィンドウが表示されます。
- ステップ 4 [電話のタイプ (Phone Type)] ドロップダウン リストから、[Cisco Collaboration モバイル コンバージェンス (Cisco Collaboration Mobile Convergence)] を選択し、[次へ (Next)] をクリックします。
[電話の設定 (Phone Configuration)] ウィンドウが表示されます。
- ステップ 5 [オーナーのユーザ ID (Owner User ID)] ドロップダウンから、デバイスを所有するエンド ユーザを選択します。
- ステップ 6 [デバイス プール (Device Pool)] ドロップダウンから、デバイス プールを選択します。
- ステップ 7 [保存 (Save)] をクリックします。
[設定の適用 (Apply Config)] ボタンをクリックして変更を有効にすることを求める警告メッセージがポップアップします。[OK] をクリックします。デバイスは正常に追加されました。
- ステップ 8 [電話番号 (Directory Number)] を設定するには、追加された CMC デバイスをクリックし、[電話番号 (Directory Number)] を入力して、[保存 (Save)] をクリックします。
- ステップ 9 追加された CMC デバイスの新しい [リモート接続先 (Remote Destination)] を追加するには、アイデンティティ ボックス内のリンクをクリックします。
- ステップ 10 [リモート接続先の設定 (Remote Destination Configuration)] ウィンドウで、[名前 (Name)]、[接続先の番号 (Destination number)] をクリックして、[保存 (Save)] をクリックします。

(注) 追加された 1 つの CMC デバイスに対して、1 つだけのリモート接続先を追加できます。
- ステップ 11 既存のリモート接続先を更新するには、[新しい名前 (New Name)] をクリックして、[保存 (Save)] をクリックします。
- ステップ 12 既存のリモート接続先を削除するには、メニューで [削除 (Delete)] ボタンをクリックします。

永続的な削除を確認する Web ページからのメッセージが表示されます。[OK] をクリックします。

ステップ 13 [デバイス (Device)] ページから CMC デバイスを削除するには、[デバイス (Device)] チェックボックスを選択し、メニューから [選択の削除 (Delete Selected)] をクリックします。

CMC RD 機能の相互作用

表 5: CMC RD 機能の相互作用

機能	連携動作
共有回線の処理	<ul style="list-style-type: none"> • CMC RD および Spark RD と関連付けられている共有デスクフォンがあるセットアップで、ユーザがエンタープライズ電話から CMC デバイス DN にコールすると、CMC RD、Spark RD、および共有デスクフォンの 3 つすべてが鳴ります。 • リモート接続先のいずれかから応答すると、共有デスクフォンに「リモートで使用 (Remote in Use)」メッセージが表示されます。 • 共有デスクフォンのいずれかから応答すると、両方のリモート接続先電話 (CMC RD と Spark RD 電話) が切断されます。
Call Manager グループ (CMG) セットアップで動作する CMC デバイス	<ul style="list-style-type: none"> • CMC デバイスが Call Manager グループに関連付けられている場合は、必ずプライマリ サーバで実行され、プライマリサーバがダウンした場合にのみ、Call Manager グループの次のアクティブなセカンダリサーバで実行されます。 • プライマリサーバがコール中にダウンした場合、進行中のコールは引き続き維持され、コールが終了した後に CMC デバイスがセカンダリサーバに登録されます。 (注) コールが保持モードの場合、電話間のメディアは引き続きアクティブですが、コールの切断を除く他の操作は実行できません。 • 最初にプライマリサーバがダウンし、CMC デバイスがセカンダリサーバに登録されているときにコールが開始され、プライマリサーバが進行中のコール中に起動した場合、コールは保持モードになり、コールの終了後に CMC デバイスがプライマリサーバに登録されます。

機能	連携動作
<p>コール アンカリング</p>	<p>CMCデバイスからのすべての基本着信コールおよび番号からリモート接続先へのコールは、エンタープライズ ネットワークでは固定されています。</p> <p>CMCのリモートデバイスが設定されている場合、エンタープライズに固定されているすべてのコールにより、ユーザはモバイルデバイスからコールを発信および受信できます。</p> <ul style="list-style-type: none"> • ユーザは、エンタープライズ番号から CMC リモート宛先に直接ダイヤルすることができます。コールはエンタープライズ ネットワークでは固定されています。このシナリオでは、デスクフォン（CMC デバイスの共有回線）は鳴りませんが、[リモートで使用（Remote in Use）] の状態のままになります。 • ユーザは、CMC リモート接続先から任意のエンタープライズ番号にダイヤルできます。コールは固定されています。このシナリオでは、デスクフォン（CMC デバイスの共有回線）は鳴りませんが、[リモートで使用（Remote in Use）] の状態のままになります。

機能	連携動作
<p>シングルナンバーリーチ</p>	<ul style="list-style-type: none"> • [リモート接続先の設定 (Remote Destination configuration)] ページで、[シングルナンバーリーチを有効にする (Enable Single Number Reach)] チェックボックスがオフになっている場合、コールは CMC RD まで拡張されず、拒否されます。 • リモート接続先からの着信コールと、[番号からリモート接続先へ (Number to Remote Destination)] の発信コールは、[シングルナンバーリーチを有効にする (Enable Single Number Reach)] チェックボックスの選択に関係なく、影響を受けません。 • CMC デバイスがある共有デスクフォンがあり、[シングルナンバーリーチを有効にする (Enable Single Number Reach)] チェックボックスがオフになっている場合、コールは CMC RD ではなく共有デスクフォンに拡張されます。 <p>(注) シングルナンバーリーチボイスメールポリシーが [ユーザ制御 (user control)] に設定されている場合、プライマリ内線番号への ブラインド転送 が発生しても、モビリティの接続先番号はトリガーされません。プライマリ内線番号のみがトリガーされます。</p> <p>ユーザ制御設定は、相談転送をサポートしていません。タイマー制御ボイスメール回避ポリシーは、相談とブラインド転送の両方をサポートします。</p>

機能	連携動作
<p>時刻（ToD）に基づくコールルーティング</p>	<ul style="list-style-type: none"> • リング スケジュールを設定するために、リモート接続先の [時刻（Time of Day）] 設定を使用できます（たとえば、月曜日から金曜日の 9 am ～ 5 pm などといった特定の時間を設定できます）。コールは、これらの時間にのみリモート接続先にリダイレクトされます。 <p>エンタープライズ電話から CMC 番号へのコールは、[リモート接続先の設定（Remote Destination configuration）] ページで修正されたリング スケジュールに基づいてルーティングされます。リング スケジュールは次のように指定できます。</p> <ul style="list-style-type: none"> • [すべての時間（All the Time）]：コールは常時ルーティングされます。制限はありません。 • [曜日（Day(s) of the week）]：選択した特定の曜日にのみコールはルーティングされます。 • [特定の時間（Specific time）]：コールは選択した就業時間内でのみルーティングされます。必ずタイムゾーンを選択します。 <ul style="list-style-type: none"> • リング スケジュール中にコールを受信する場合、エンタープライズ電話から CMC 番号へのコールは、[リモート接続先の設定（Remote Destination configuration）] ページでアクセス許可リストまたはアクセスブロッキングリストに追加されたコール番号またはパターンに基づいてルーティングされます。 <ul style="list-style-type: none"> • [アクセス許可リスト（Allowed access list）]：発信者番号またはパターンがアクセス許可リスト内にある場合にのみ接続先が鳴ります。 • [アクセスブロッキングリスト（Blocked access list）]：発信者番号またはパターンがアクセスブロッキングリスト内にある場合には接続先は鳴りません。 <p>(注) 任意の時点で、アクセス許可リストまたはアクセスブロッキングリストのみを使用できます。</p>

機能	連携動作
<p>ユーザ ロケールの設定</p>	<p>CMC 仮想デバイスでは、[電話の設定 (Phone Configuration)] ウィンドウで設定されているロケール設定を使用して、電話のディスプレイと電話アナウンスのロケールを判断します。このポリシーは、通常のコールと Conference Now 番号に適用されます。</p> <p>アナウンスの部分は、[ユーザ ロケール (User Locale)] の設定で同じ言語が選択された発信側 (任意のエンタープライズ電話) および着信側 (CMC デバイス) 電話では、発信側とリモート接続先の両方のアナウンスは、[電話の設定 (Phone Configuration)] ページで選択された [ユーザ ロケール (User Locale)] 設定に基づくものになります。</p> <p>(注) たとえば、CMC デバイスに関連付けられている [リモート接続先 (Remote Destination)] から [Conference Now 番号 (Conference Now 番号)] に発信するとき、アナウンスは CMC デバイスの [電話の設定 (Phone configuration)] ページで選択されている [ユーザ ロケール (User Locale)] の設定に基づくものになります。</p>
<p>HLogin および HLogout の新しいアクセス コード</p>	<p>この機能は、管理者が追加のサービス パラメータを使用して、CMC デバイスのハントグループのログインおよびログアウト数を設定するために役立ちます。</p> <ul style="list-style-type: none"> • ハントグループログインのためのエンタープライズ機能アクセス番号。 • ハントグループログアウトのためのエンタープライズ機能アクセス番号。 <p>ユーザが CMC デバイスに関連付けられている RD から Hlogin 番号を入力すると、そのときに限りコールは CMC デバイスに関連付けられているハントパイロット番号のダイヤル時に RD にリダイレクトされます。</p> <p>ユーザが CMC デバイスに関連付けられている RD から Hlogout 番号を入力すると、コールは CMC デバイスに関連付けられているハントパイロット番号のダイヤル時に RD にリダイレクトされません。</p> <p>デフォルトでは、CMC デバイスは Hloggedin です。いずれの場合でも、CMC デバイスへの直接コールには影響はありません。</p>

機能	連携動作
<p>データベースに設定された [呼び出し前の遅延タイマー (Delay Before Ringing Timer)] に基づく CMC リモート接続先コールエクステンション</p>	<p>DB の [呼び出し前の遅延タイマー (Delay Before Ringing Timer)] が 5000 に設定されている場合</p> <ul style="list-style-type: none"> • エンタープライズ電話から CMC 番号に発信する場合、共有回線が鳴り、コールは5秒後にリモート接続先に到達します。 • エンタープライズ電話から CMC 番号に発信する場合、共有回線が 5 秒前にコールに応答すると、コールはリモート接続先に拡張されません。 • エンタープライズ電話から CMC 番号に発信する場合、共有回線が鳴り、発信側が 5 秒前にコールを切断すると、コールはリモート接続先に拡張されません。 <p>DB の [呼び出し前の遅延タイマー (Delay Before Ringing Timer)] が 0 に設定されている場合</p> <p>エンタープライズ電話から CMC 番号へのすべてのコールは、リモート接続先と共有回線に同時にアラートを出します。</p>
<p>一括管理ツール (BAT) サポート</p>	<p>BAT サポートは CMC デバイス向けに提供されています</p>

CMC RD 機能の制約事項

表 6: CMC RD 機能の制約事項

機能	制約事項
CMC リモート接続先の関連付け	<p>次の制約事項が適用されます。</p> <ul style="list-style-type: none"> • CMC デバイスには、1 つのリモート接続先のみを関連付けることができます。 • エンドユーザが削除されると、その関連付けられている CMC デバイスおよび RD (リモート接続先) も削除されます。 <p>(注) [モビリティの有効化 (Enable Mobility)]チェックボックスがオンまたはオフになっていても、CMC および RD は影響を受けません。CMC デバイスは削除されません。</p> <p>(注) Cisco Unified Communications Manager は、CMC デバイスのコールハンドルの保存をサポートしていません。</p>

既存の電話機の移動

次の手順を実行して、設定された電話機をエンドユーザに移動します。

手順

- ステップ 1 Cisco Unified CM の管理で、[ユーザ管理 (User Management)]>[ユーザ/電話の追加 (User/Phone Add)]>[ユーザ/電話のクイック追加 (Quick User/Phone Add)]を選択します。
- ステップ 2 [検索 (Find)]をクリックして、既存の電話機を移動するユーザを選択します。
- ステップ 3 [デバイスの管理 (Manage Devices)] ボタンをクリックします。
- ステップ 4 [このユーザに移動する電話の検索 (Find a Phone to Move To This User)] ボタンをクリックします。
- ステップ 5 このユーザに移動する電話機を選択します。
- ステップ 6 [選択項目の移動 (Move Selected)] をクリックします。

現在ログイン中のデバイスの検索

Cisco Extension Mobility 機能と Cisco Extension Mobility Cross Cluster 機能により、ユーザが現在ログインしているデバイスの記録が維持されます。Cisco Extension Mobility 機能では、現在ログイン中のデバイスのレポートでローカルユーザが現在ログインしているローカル電話が追跡され、Cisco Extension Mobility Cross Cluster 機能では、現在ログイン中のデバイスのレポートでリモートユーザが現在ログインしているローカル電話が追跡されます。

Unified Communications Manager には、ユーザがログインしているデバイスを検索するための特定の検索ウィンドウがあります。特定のデバイスを検索する場合、またはユーザが現在ログインしているすべてのデバイスを一覧表示する場合は、次の手順に従います。

手順

ステップ 1 [デバイス (Device)] > [電話 (Phone)] の順に選択します。

ステップ 2 右上隅にある [関連リンク (Related Links)] ドロップダウンリストから [現在ログイン中のデバイスのレポート (Actively Logged In Device Report)] を選択し、[移動 (Go)] をクリックします。

ステップ 3 現在ログイン中のすべてのデバイスレコードをデータベースで検索するには、ダイアログボックスが空であることを確認して、ステップ 4 に進みます。

レコードをフィルタまたは検索するには、次の手順を実行します。

- 最初のドロップダウンリストで、検索パラメータを選択します。
- 2 番目のドロップダウンリストで、検索パターンを選択します。
- 必要に応じて、適切な検索テキストを指定します。

(注) 検索条件をさらに追加するには、[+] ボタンをクリックします。条件を追加すると、指定した条件をすべて満たしているレコードが検索されます。条件を削除する場合、最後に追加した条件を削除するには、[-] ボタンをクリックします。追加した検索条件をすべて削除するには、[フィルタのクリア (Clear Filter)] ボタンをクリックします。

ステップ 4 [検索 (Find)] をクリックします。

条件を満たしているレコードがすべて表示されます。1 ページあたりの項目の表示件数を変更するには、[ページあたりの行数 (Rows per Page)] ドロップダウンリストで別の値を選択します。

ステップ 5 表示されるレコードのリストで、表示するレコードのリンクをクリックします。

(注) ソート順を反転させるには、リスト見出しの上矢印または下矢印が使用可能であればそれをクリックします。

選択した項目がウィンドウに表示されます。

リモートログインデバイスの検索

Cisco Extension Mobility Cross Cluster 機能は、ユーザがリモートログインしているデバイスのレコードを保持します。リモートログインデバイス レポートによって追跡される電話機は、他のクラスタが所有しており、かつ EMCC 機能を使用するローカルユーザが現在ログインしているものとなります。

Unified Communications Manager には、ユーザがリモートログインしているデバイスを検索するための特定の検索ウィンドウがあります。次の手順に従って、特定のデバイスを検索したり、ユーザがリモートでログインしているすべてのデバイスを列挙したりします。

手順

ステップ 1 [デバイス (Device)] > [電話 (Phone)] の順に選択します。

ステップ 2 右上にある [関連リンク (Related Links)] ドロップダウンリストで [リモートログインデバイス (Remotely Logged In Device)] を選択し、[移動 (Go)] をクリックします。

ステップ 3 データベース内のすべてのリモートログインデバイスのレコードを検索するには、ダイアログボックスが空であることを確認して、ステップ 4 に進みます。

レコードをフィルタまたは検索するには、次の手順を実行します。

- a) 最初のドロップダウンリストで、検索パラメータを選択します。
- b) 2 番目のドロップダウンリストで、検索パターンを選択します。
- c) 必要に応じて、適切な検索テキストを指定します。

(注) 検索条件をさらに追加するには、[+] ボタンをクリックします。条件を追加すると、指定した条件をすべて満たしているレコードが検索されます。条件を削除する場合、最後に追加した条件を削除するには、[-] ボタンをクリックします。追加した検索条件をすべて削除するには、[フィルタのクリア (Clear Filter)] ボタンをクリックします。

ステップ 4 [検索 (Find)] をクリックします。

条件を満たしているレコードがすべて表示されます。1 ページあたりの項目の表示件数を変更するには、[ページあたりの行数 (Rows per Page)] ドロップダウンリストで別の値を選択します。

ステップ 5 表示されるレコードのリストで、表示するレコードのリンクをクリックします。

(注) ソート順を反転させるには、リスト見出しの上矢印または下矢印が使用可能であればそれをクリックします。

選択した項目がウィンドウに表示されます。

電話機のリモートロック

一部の電話機は、リモートでロックすることができます。電話機をリモートでロックすると、ロックを解除するまで使用できなくなります。

電話機でリモートロック機能がサポートされている場合は、右上の隅に[ロック (Lock)]ボタンが表示されます。

手順

ステップ1 [デバイス (Device)] > [電話 (Phone)] の順に選択します。

ステップ2 [電話の検索/一覧表示 (Find and List Phones)] ウィンドウから、検索条件を入力し、[検索 (Find)] をクリックして特定の電話機を見つけます。

検索条件に一致する電話機のリストが表示されます。

ステップ3 リモートロックを実行する電話機を選択します。

ステップ4 [電話の設定 (Phone Configuration)] ウィンドウで[ロック (Lock)] をクリックします。

電話機が登録されていない場合は、電話機が次回登録されたときにロックされることを伝えるポップアップウィンドウが表示されます。[ロック (Lock)] をクリックします。

[デバイスのロック/ワイプのステータス (Device Lock/Wipe Status)] セクションが表示され、最新の要求、保留中かどうか、および最新の確認応答に関する情報が示されます。

工場出荷時の初期状態への電話機のリセット

一部の電話機では、リモートワイプ機能がサポートされます。リモートで電話機をワイプすると、電話機が工場出荷時の設定にリセットされます。電話機に以前に保存されたすべてのデータが消去されます。

電話機でリモートワイプ機能がサポートされている場合は、右上の隅に[ワイプ (Wipe)]ボタンが表示されます。



注意 この操作は取り消すことができません。この操作は、確実に電話機を工場出荷時の設定にリセットする必要がある場合にのみ、実行してください。

手順

ステップ1 [デバイス (Device)] > [電話 (Phone)] の順に選択します。

ステップ2 [電話の検索/一覧表示 (Find and List Phones)] ウィンドウで、検索条件を入力し、[検索 (Find)] をクリックして特定の電話機を見つけます。

検索条件に一致する電話機のリストが表示されます。

ステップ 3 リモートワイプを実行する電話機を選択します。

ステップ 4 [電話の設定 (Phone Configuration)] ウィンドウで [ワイプ (Wipe)] をクリックします。

電話機が登録されていない場合は、電話機が次回登録されたときにワイプされることを伝えるポップアップウィンドウが表示されます。[ワイプ (Wipe)] をクリックします。

[デバイスのロック/ワイプのステータス (Device Lock/Wipe Status)] セクションが表示され、最新の要求、保留中かどうか、および最新の確認応答に関する情報が示されます。

電話ロック/ワイプレポート

Unified Communications Manager には、リモートでロックまたはリモートでワイプされたデバイスを検索するための特定の検索ウィンドウがあります。次の手順に従って、特定のデバイスを検索したり、リモートでロックされたまたはリモートでワイプされたすべてのデバイスを列挙したりします。

手順

ステップ 1 [デバイス (Device)] > [電話 (Phone)] の順に選択します。

[電話の検索/一覧表示 (Find and List Phones)] ウィンドウが表示されます。このウィンドウには、アクティブな (以前の) クエリーのレコードも表示されることがあります。

ステップ 2 ウィンドウの右上にある [関連リンク (Related Links)] ドロップダウンリストで [電話のロック/ワイプレポート (Phone Lock/Wipe Report)] を選択し、[移動 (Go)] をクリックします。

ステップ 3 データベース内のリモートでロックされたデバイスまたはリモートでワイプされたデバイスのすべてのレコードを検索するには、テキストボックスが空であることを確認して、ステップ 4 に進みます。

特定のデバイスのレコードを絞り込むまたは検索するには：

- 1 つ目のドロップダウンリストで、検索するデバイス稼働タイプを選択します。
- 2 番目のドロップダウンリストで、検索パラメータを選択します。
- 3 番目のドロップダウンリストで、検索パターンを選択します。
- 必要に応じて、適切な検索テキストを指定します。

(注) 検索条件をさらに追加するには、[+] ボタンをクリックします。条件を追加すると、指定した条件をすべて満たしているレコードが検索されます。条件を削除する場合、最後に追加した条件を削除するには、[-] ボタンをクリックします。追加した検索条件をすべて削除するには、[フィルタのクリア (Clear Filter)] ボタンをクリックします。

ステップ 4 [検索 (Find)] をクリックします。

条件を満たしているレコードがすべて表示されます。1 ページあたりの項目の表示件数を変更するには、[ページあたりの行数 (Rows per Page)] ドロップダウンリストで別の値を選択します。

ステップ 5 表示されるレコードのリストで、表示するレコードのリンクをクリックします。

(注) ソート順を反転させるには、リスト見出しの上矢印または下矢印が使用可能であればそれをクリックします。

選択した項目がウィンドウに表示されます。

電話の LSC ステータスの表示および CAPF レポートの生成

この手順を使用して、Cisco Unified Communications Manager インタフェース内からローカルで有効な証明書 (LSC) の有効期限情報を監視します。次の検索フィルタは、LSC 情報を表示します。

- [LSC 有効期日 (LSC Expires)] : 電話の LSC 有効期日を表示します。
- [LSC 発行元 (LSC Issued By)] : 発行元の名前を表示します。これは、CAPF またはサードパーティのいずれかです。
- [LSC 発行元の有効期日 (LSC Issuer Expires By)] : 発行元の有効期日を表示します。



(注) 新しいデバイスに LSC が発行されていない場合、[LSC 有効期日 (LSC Expires)] および [LSC 発行元の有効期日 (LSC Issuer Expires by)] フィールドのステータスは [該当なし (NA)] 「」に設定されます。

Cisco Unified Communications Manager 11.5(1) へのアップグレード前に LSC がデバイスに発行された場合は、[LSC 有効期日 (LSC Expires)] および [LSC 発行元の有効期日 (LSC Issuer Expires by)] フィールドのステータスは [不明 (Unknown)] 「」に設定されます。

手順

ステップ 1 [デバイス (Device)] > [電話 (Phone)] の順に選択します。

ステップ 2 [電話の検索条件 (Find Phone where)] の最初のドロップダウンリストから、次の基準の 1 つを選択します。

- LSC 有効期日 (LSC Expires)
- LSC 発行元 (LSC Issued By)
- LSC 発行元の有効期日 (LSC Issuer Expires by)

[電話の検索条件 (Find Phone where)] の 2 番目のドロップダウンリストから、次の基準の 1 つを選択します。

- ~が次の日付より前 (is before)
- 次の文字列と完全に一致する
- ~が次の日付より後
- ~で始まる
- ~を含む
- ~が次の文字列で終わる
- 次の文字列と完全に一致する
- 空である
- ~が空ではない

ステップ 3 [検索 (Find)] をクリックします。
検出された電話の一覧が表示されます。

ステップ 4 [関連リンク (Related Links)] ドロップダウンリストから [ファイルでの CAPF レポート (CAPF Report in File)] を選択し、[移動 (Go)] をクリックします。
レポートがダウンロードされます。



第 8 章

デバイス ファームウェアの管理

- デバイス ファームウェアのアップデートの概要 (93 ページ)
- デバイス パックまたは個々のファームウェアのインストール (94 ページ)
- システムからの未使用のファームウェアの削除 (96 ページ)
- 電話モデルのデフォルト ファームウェアの設定 (97 ページ)
- 電話のファームウェア ロードの設定 (98 ページ)
- ロード サーバの使用 (99 ページ)
- 非デフォルト ファームウェア ロードを使用するデバイスの検索 (100 ページ)

デバイス ファームウェアのアップデートの概要

デバイス ロードとは、IP Phone、Telepresence Systems、および Cisco Unified Communications Manager でプロビジョニングおよび登録されているその他のデバイスを対象としたソフトウェアおよびファームウェアのことです。Cisco Unified Communications Manager はインストールまたはアップグレード時に、Cisco Unified Communications Manager の該当するバージョンがリリースされた時期に基づいて、利用可能な最新のロードをインクルードします。シスコでは、新しい機能やソフトウェア フィックスを導入するために更新されたファームウェアを定期的にリリースしています。したがって、新しいロードをインクルードした Cisco Unified Communications Manager アップグレードを待たずに、電話機を新しいロードに更新することができます。

エンドポイントをソフトウェアの新しいバージョンにアップグレードするには、エンドポイントがアクセス可能な場所に新しいロードに必要なファイルがダウンロード可能になっていなければなりません。最も一般的な場所は、Cisco TFTP サービスがアクティブにされている、「TFTP サーバ」と呼ばれる Cisco UCM ノードです。一部の電話機は、「ロードサーバ」と呼ばれる別のダウンロード場所もサポートしています。

任意のサーバ上の tftp ディレクトリ内にあるファイルのリストを取得したり、それらのファイルを表示またはダウンロードしたりするには、CLI コマンドの `file list tftp` (tftp ディレクトリ内のファイルを一覧表示する場合)、`file view tftp` (ファイルを表示する場合)、`file get tftp` (tftp ディレクトリ内のファイルのコピーを取得する場合) を使用します。詳細については、

『*Command Line Interface Reference Guide for Cisco Unified Communications Solutions*』を参照してください。また、Web ブラウザで URL 「`http://<tftp_server>:6970/<filename>`」 にアクセスして、任意の TFTP ファイルをダウンロードすることもできます。



ヒント 新しいロードをシステム全体のデフォルトとして設定する前に、単一のデバイスに新規ロードを適用することもできます。この手法は、テスト目的で役立ちます。ただし、該当するタイプのその他すべてのデバイスは、新しいロードでシステム全体のデフォルトを更新するまでは、古いロードを使用することに注意してください。

デバイス パックまたは個々のファームウェアのインストール

デバイス パッケージをインストールして、新しい電話タイプを導入し、複数の電話モデルのファームウェアをアップグレードします。

- 既存のデバイスの個々のファームウェアは次のオプションでインストールまたはアップグレードできます。Cisco Options Package (COP) ファイル：COP ファイルには、ファームウェア ファイルとデータベース アップデートが含まれています。このためパブリッシャにインストールすると、ファームウェアファイルがインストールされ、さらにデフォルトのファームウェアが更新されます。
- ファームウェアファイルのみ：zipファイルで提供されます。zipファイルに含まれている個々のデバイスファームウェアファイルは手動で解凍し、TFTPサーバの適切なディレクトリにおよびアップロードする必要があります。



(注) COP またはファームウェア ファイル パッケージに固有のインストール手順については、README ファイルを参照してください。

手順

- ステップ 1** Cisco Unified OS の管理から、[ソフトウェア アップグレード (Software Upgrades)] > [インストール/アップグレード (Install/Upgrade)] の順に選択します。
- ステップ 2** ソフトウェアの場所セクションに適切な値を入力し、[次へ (Next)] をクリックします。
- ステップ 3** [使用可能なソフトウェア (Available Software)] ドロップダウンリストで、デバイスパッケージファイルを選択して、[次へ (Next)] をクリックします。
- ステップ 4** MD5 の値が正しいことを確認し、[次へ (Next)] をクリックします。
- ステップ 5** 警告ボックスで、正しいファームウェアを選択したことを確認し、[インストール (Install)] をクリックします。
- ステップ 6** 成功メッセージを受信したことを確認します。

(注) クラスタを再起動している場合は、ステップ 8 に進みます。

- ステップ7 サービスを実行しているすべてのノードで [Cisco TFTP] サービスを再起動します。
- ステップ8 新しいロードにデバイスをアップグレードするには、影響を受けたデバイスをリセットします。
- ステップ9 Cisco Unified CM の管理から、[デバイス (Device)]> [デバイスの設定 (Device Settings)]> [デバイスのデフォルト (Device Defaults)] の順に選択し、新しいロードに (特定のデバイスに対して) ロード ファイルの名前を手動で変更します。
- ステップ10 [保存 (Save)] をクリックし、デバイスをリセットします。
- ステップ11 すべてのクラスタ ノードで **Cisco Tomcat** サービスを再起動します。
- ステップ12 次のいずれかを実行します。
 - 11.5(1)SU4 以下、12.0(1)、または 12.0(1)SU1 を実行している場合は、クラスタを再起動します。
 - 11.5(1)SU5 以上での 11.5(x) リリース、12.0(1)SU2 以上での任意のリリースを実行している場合は、パブリッシャ ノード上で **Cisco CallManager** サービスを再起動します。ただし、サブスクリバ ノードでのみ **Cisco CallManager** サービスを実行している場合は、このタスクをスキップできます。

ファームウェアのインストールの潜在的な問題

デバイスパックのインストール後に発生する可能性があるいくつかの潜在的な問題を次に示します。

問題	原因/解決
新しいデバイスが登録されません	<p>これはデバイス タイプの不一致により発生する可能性があります。次の原因が考えられます。</p> <ul style="list-style-type: none"> • デバイスが [電話の設定 (Phone Configuration)] ウィンドウで、不適切なデバイス タイプを使用して追加されました。たとえば、Cisco DX80 が Cisco TelePresence DX80 ではなく電話タイプとして選択されました。適切なデバイス タイプを使用して、デバイスを再設定します。 • Cisco CallManager サービスが新しいデバイス タイプを認識しません。この場合、パブリッシャ ノード上で Cisco CallManager サービスを再起動します。
エンドポイントが新しいファームウェアにアップグレードしません	<p>Possible reasons:</p> <ul style="list-style-type: none"> • デバイスパックが TFTP サーバにインストールされていません。その結果、ファームウェアは電話機でダウンロードできません。 • Cisco TFTP サービスは、インストール後に再起動されなかったため、新しいファイルについて認識しません。必ず TFTP サーバにデバイスパックをインストールします。

問題	原因/解決
<p>Cisco Unified CM Administration の [電話の設定 (Phone Configuration)] ウィンドウで、新しいデバイス タイプのアイコン イメージがあるはずの場所に、破損したリンクが表示されます。</p>	<p>CLI からすべてのノードで Cisco Tomcat サービスを再起動します。</p>
<p>エンドポイントのファームウェアのダウンロードが途中で失敗したり、ダウンロード全体が再起動したり、ダウンロードが非常に遅いように見えます。</p> <p>重要 リリース 14SU1 以降に適用されます。</p>	<p>Possible reasons:</p> <p>これは、ネットワークの問題または輻輳が原因である可能性が高く、一括アップグレードのシナリオでより一般的である可能性があります。</p> <p>14SU1 を実行している場合、TFTP およびプロキシ TFTP での HTTP 範囲リクエスト (RFC7233) のサポートを利用できる可能性があります (ダウンロードファイルが少なくとも 100MB の場合)。</p> <p>HTTP 範囲リクエストをサポートするエンドポイントは、特に電話の一括アップグレードシナリオやネットワーク状態が悪い場合に、信頼性とダウンロード速度の向上によるメリットを得ることができます。</p> <p>HTTP 範囲リクエストでは、ダウンロードの一時停止と再開を許可する必要があります。つまり、中断されたダウンロードは、ダウンロード全体を再度やり直すことなく、最後に成功したことがわかっているバイト範囲から続行できます。</p> <p>Cisco Webex Wireless Phone 840 および 860 (RFC7233 サポート)。 RFC7233 をサポートしていないデバイスは、この機能の影響を受けません。</p>

システムからの未使用のファームウェアの削除

[デバイス ロード管理 (Device Load Management)] ウィンドウでは、システムから未使用のファームウェア (デバイスロード) および関連するファイルを削除して、ディスク容量を増やすことができます。たとえば、アップグレード前に未使用のロードを削除して、ディスク容量の不足が原因でアップグレードが失敗しないようにすることができます。ファームウェアファイルの中には、[デバイス ロード管理 (Device Load Management)] ウィンドウにリストされない依存ファイルを持っているものがあります。ファームウェアを削除すると、依存ファイルも削除されます。ただし、その依存ファイルが他のファームウェアに関連付けられている場合は削除されません。



(注) クラスタ内の各サーバで、個別に未使用のファームウェアを削除する必要があります。

始める前に



注意 未使用のファームウェアを削除する前に、適切なロードを削除していることを確認します。削除されたロードは、クラスタ全体の DRS 復元を実行しないと復元できません。ファームウェアを削除する前にバックアップすることを推奨します。

複数のファイルのロードを使用するデバイスのファイルを削除しないようにしてください。たとえば、特定の CE エンドポイントは複数のロードを使用します。ただし、**[デバイス ロード管理 (Device Load Management)]** ウィンドウで **[使用中 (In Use)]** として参照されるロードは 1 つだけです。

手順

- ステップ 1** [Cisco Unified OS の管理 (Cisco Unified OS Administration)] から、[ソフトウェア アップグレード (Software Upgrades)] > [デバイス ロード管理 (Device Load Management)] の順に選択します。
- ステップ 2** 検索条件を指定して、[検索 (Find)] をクリックします。
- ステップ 3** 削除するデバイス ロードを選択します。必要な場合は、複数のロードを選択できます。
- ステップ 4** [選択されたロードの削除 (Delete Selected Loads)] をクリックします。
- ステップ 5** [OK] をクリックします。

電話モデルのデフォルト ファームウェアの設定

この手順を使用して、特定の電話モデルにデフォルトのファームウェアロードを設定します。新しい電話が登録されると、Cisco Unified Communications Manager は、[電話の設定 (Phone Configuration)] ウィンドウでデフォルトを上書きするファームウェア ロードが指定されていないかぎり、デフォルトのファームウェアを電話に送信しようとします。



(注) 個々の電話については、[電話の設定 (Phone Configuration)] ウィンドウの [電話ロード名 (Phone Load Name)] フィールドの設定により、その特定の電話のデフォルト ファームウェア ロードが上書きされます。

始める前に

ファームウェアが TFTP サーバにロードされていることを確認します。

手順

-
- ステップ 1 [Cisco Unified CM の管理 (Cisco Unified CM Administration)] > [デバイス (Device)] > [デバイスの設定 (Device Settings)] > [デバイスのデフォルト (Device Defaults)] を選択します。
[デバイスのデフォルト設定 (Device Defaults Configuration)] ウィンドウが表示され、Cisco Unified Communications Manager がサポートする様々な電話モデルのデフォルト ファームウェア ロードが示されます。ファームウェアは [ロード情報 (Load Information)] 列に表示されます。
 - ステップ 2 [デバイス タイプ (Device Type)] で、デフォルト ファームウェアを割り当てる電話モデルを指定します。
 - ステップ 3 横にある [ロード情報 (Load Information)] フィールドに、ファームウェア ロードを入力します。
 - ステップ 4 (任意) [デバイス プール (Device Pool)] にデフォルトのデバイス プールを入力し、[電話 テンプレート (Phone Template)] に該当する電話モデルのデフォルトの電話テンプレートを入力します。
 - ステップ 5 [保存 (Save)] をクリックします。
-

電話のファームウェア ロードの設定

この手順を使用して、特定の電話にファームウェア ロードを割り当てます。[デバイスのデフォルト設定 (Device Defaults Configuration)] ウィンドウに指定されているデフォルトとは異なるファームウェア ロードを使用する場合に、この手順を実行します。



-
- (注) 多数の電話に1つのバージョンを割り当てる場合は、一括管理ツールを使用し、CSVファイルまたはクエリを使用して、[電話ロード名 (Phone Load Name)] フィールドを設定できます。詳細については、『*Bulk Administration Guide for Cisco Unified Communications Manager*』を参照してください。
-

手順

-
- ステップ 1 Cisco Unified CM Administration で、[デバイス (Device)] > [電話 (Phone)] を選択します。
 - ステップ 2 [検索 (Find)] をクリックし、個別の電話を選択します。
 - ステップ 3 [電話ロード名 (Phone Load Name)] フィールドに、ファームウェアの名前を入力します。この電話では、ここで指定したファームウェア ロードによって、[デバイスのデフォルト設定

(Device Defaults Configuration)] ウィンドウで指定されているデフォルトのファームウェアロードが上書されます。

- ステップ 4 [電話の設定 (Phone Configuration)] ウィンドウで、残りのフィールドを入力します。フィールドとその設定の詳細については、オンラインヘルプを参照してください。
- ステップ 5 [保存 (Save)] をクリックします。
- ステップ 6 [設定の適用 (Apply Config)] をクリックして、変更したフィールドを電話にプッシュします。

ロードサーバの使用

電話が TFTP サーバ以外のサーバからファームウェアの更新をダウンロードするようにするには、電話の [電話の設定 (Phone Configuration)] ページで「ロードサーバ」を設定できます。ロードサーバには、別の Cisco Unified Communications Manager またはサードパーティのサーバを指定できます。サードパーティのサーバは、電話が TCP ポート 6970 で HTTP を使用して（推奨）、または UDP ベースの TFTP プロトコルを使用して要求するすべてのファイルを提供する必要があります。DX ファミリの Cisco TelePresence デバイスなどの一部の電話モデルでは、ファームウェアのアップデートで HTTP のみをサポートしています。



- (注) 多数の電話に 1 つのロードサーバを割り当てる場合は、一括管理ツールを使用し、CSV ファイルまたはクエリを使用して、[ロードサーバ (Load Server)] フィールドを設定できます。詳細については、『*Bulk Administration Guide for Cisco Unified Communications Manager*』を参照してください。

手順

- ステップ 1 Cisco Unified CM Administration で、[デバイス (Device)] > [電話 (Phone)] を選択します。
- ステップ 2 [検索 (Find)] をクリックし、個別の電話を選択します。
- ステップ 3 [ロードサーバ (Load Server)] フィールドに、別のサーバの IP アドレスまたはホスト名を入力します。
- ステップ 4 [電話の設定 (Phone Configuration)] ウィンドウで、残りのフィールドを入力します。フィールドとその設定の詳細については、オンラインヘルプを参照してください。
- ステップ 5 [保存 (Save)] をクリックします。
- ステップ 6 [設定の適用 (Apply Config)] をクリックして、変更したフィールドを電話にプッシュします。

非デフォルトファームウェアロードを使用するデバイスの検索

Unified Communications Manager の [ファームウェアロード情報 (Firmware Load Information)] ウィンドウを使用すると、デバイス タイプ用のデフォルトファームウェアロードを使用していないデバイスをすばやく特定できます。



(注) 各デバイスには、デフォルトをオーバーライドする個別のファームウェアロードを割り当てる
ことができます。

デフォルトファームウェアロードを使用していないデバイスを特定するには、次の手順に従います。

手順

ステップ 1 [デバイス (Device)] > [デバイスの設定 (Device Settings)] > [ファームウェアロード情報 (Firmware Load Information)] の順に選択します。

ページが更新され、ファームウェアロードが必要なデバイスタイプが一覧表示されます。デバイスタイプごとに、[デフォルトロードを使用しないデバイス (Devices Not Using Default Load)] 列が、非デフォルトロードを使用するデバイスの設定にリンクされます。

ステップ 2 非デフォルトデバイスロードを使用する特定のデバイスタイプのデバイスのリストを表示するには、[デフォルトロードを使用しないデバイス (Devices Not Using Default Load)] 列でそのデバイスタイプのエントリをクリックします。

開いたウィンドウに、デフォルトファームウェアロードを実行していない特定のデバイスタイプのデバイスが一覧表示されます。



第 9 章

インフラストラクチャ デバイスの管理

- [インフラストラクチャの管理の概要 \(101 ページ\)](#)
- [インフラストラクチャの管理の前提条件 \(101 ページ\)](#)
- [インフラストラクチャの管理のタスク フロー \(102 ページ\)](#)

インフラストラクチャの管理の概要

この章では、ロケーション対応機能の一部として、スイッチとワイヤレスアクセスポイントなどのネットワーク インフラストラクチャ デバイスを管理するタスクについて説明します。ロケーション対応を有効にすると、Cisco Unified Communications Manager データベースには、各スイッチまたはアクセスポイントに現在関連付けられているエンドポイントのリストを含め、ネットワークのスイッチとアクセスポイントのステータス情報が保存されます。

エンドポイントからインフラストラクチャ デバイスへのマッピングは、Cisco Unified Communications Manager と Cisco Emergency Responder が発信者の物理的な場所を特定するのに役立ちます。たとえば、モバイルクライアントがローミング中に緊急通報を行っている場合、Cisco Emergency Responder はこのマッピングを使用して緊急サービスを送る場所を判断します。

データベースに保存されるインフラストラクチャ情報も、インフラストラクチャの使用状況をモニタするのに役立ちます。Unified Communications Manager インターフェイスから、スイッチやワイヤレス アクセスポイントなどのネットワーク インフラストラクチャのデバイスを確認できます。現時点で特定のアクセスポイントまたはスイッチに関連付けられているエンドポイントのリストを表示することもできます。インフラストラクチャ デバイスが使用されていない場合は、インフラストラクチャ デバイスを非アクティブ化して追跡されないようにできます。

インフラストラクチャの管理の前提条件

Cisco Unified Communications Manager インターフェイス内でワイヤレス インフラストラクチャを管理するには、その前に、ロケーション認識機能を設定する必要があります。有線インフラストラクチャの場合、この機能はデフォルトで有効になっています。

設定の詳細については、[Cisco Unified Communications Manager 機能設定ガイド](#)の「ロケーション認識の設定」の章を参照してください。

また、ネットワークインフラストラクチャをインストールする必要もあります。詳細については、ワイヤレス LAN コントローラ、アクセス ポイント、スイッチなどのインフラストラクチャ デバイスに付属しているハードウェア ドキュメントを参照してください。

インフラストラクチャの管理のタスク フロー

次のタスクを実行して、ネットワーク インフラストラクチャ デバイスを監視および管理します。

手順

	コマンドまたはアクション	目的
ステップ 1	インフラストラクチャデバイスのステータスの表示 (102 ページ)	ワイヤレス アクセス ポイントまたはイーサネット スwitchの現在のステータスを、関連付けられているエンドポイントの一覧とともに取得します。
ステップ 2	インフラストラクチャ デバイス トラッキングの非アクティブ化 (103 ページ)	使用されていないスイッチまたはアクセス ポイントがある場合は、そのデバイスに非アクティブのマークを付けます。そのインフラストラクチャ デバイスのステータスまたは関連付けられているエンドポイントの一覧が更新されなくなります。
ステップ 3	非アクティブ化されたインフラストラクチャ デバイス トラッキングのアクティブ化 (104 ページ)	非アクティブなインフラストラクチャ デバイスのトラッキングを開始します。Cisco Unified Communications Manager が、インフラストラクチャ デバイスのステータスおよび関連付けられているエンドポイントの一覧により、データベースの更新を開始します。

インフラストラクチャ デバイスのステータスの表示

この手順を使用して、ワイヤレス アクセス ポイントやイーサネット スwitchなどのインフラストラクチャ デバイスの現在のステータスを取得します。Cisco Unified Communications Manager インターフェイス内で、アクセス ポイントまたはスイッチのステータスおよび現在関連付けられているエンドポイントの一覧を表示できます。

手順

- ステップ 1 Cisco Unified CM の管理で、**[詳細機能 (Advanced Features)]** > **[デバイスの位置のトラッキング サービス (Device Location Tracking Services)]** > **[スイッチとアクセス ポイント (Switches and Access Points)]** 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 ステータスを表示するスイッチまたはアクセス ポイントをクリックします。
[スイッチおよびアクセス ポイントの設定 (Switches and Access Point Configuration)] ウィンドウに、そのアクセスポイントまたはスイッチに現在関連付けられているエンドポイントの一覧を含み、現在のステータスが表示されます。

インフラストラクチャ デバイス トラッキングの非アクティブ化

スイッチやアクセス ポイントなどの特定のインフラストラクチャ デバイスのトラッキングを削除するには、次の手順を使用します。使用されていないスイッチまたはアクセス ポイントで、この手順を実行できます。



- (注) インフラストラクチャ デバイスのトラッキングを削除すると、デバイスはデータベースに残ったまま、非アクティブになります。Cisco Unified Communications Manager は、その後、そのインフラストラクチャ デバイスに関連するエンドポイントの一覧も含めて、そのデバイスのステータスを更新しません。[スイッチとアクセスポイント (Switches and Access Points)] ウィンドウの**[関連リンク (Related Links)]** ドロップダウンで、非アクティブなスイッチとアクセスポイントを表示できます。

手順

- ステップ 1 Cisco Unified CM Administration で、**[詳細機能 (Advanced Features)]** > **[デバイスの位置のトラッキング サービス (Device Location Tracking Services)]** > **[スイッチとアクセスポイント (Switches and Access Points)]** を選択します。
- ステップ 2 **[検索 (Find)]** をクリックして、追跡を停止するスイッチまたはアクセスポイントを選択します。
- ステップ 3 **[選択項目の非アクティブ化 (Deactivate Selected)]** をクリックします。

非アクティブ化されたインフラストラクチャ デバイス トラッキングのアクティブ化

この手順を使用して、非アクティブ化されたインフラストラクチャデバイスのトラッキングを開始します。スイッチまたはアクセス ポイントがアクティブになると、Cisco Unified Communications Manager では、スイッチまたはアクセス ポイントに関連付けられているエンドポイントの一覧を含むステータスを動的にトラッキングし始めます。

始める前に

Location Awareness を設定する必要があります。詳細については、『*System Configuration Guide for Cisco Unified Communications Manager*』の「Location Awareness」の章を参照してください。

手順

-
- ステップ 1 Cisco Unified CM の管理で、**[詳細機能 (Advanced Features)]** > **[デバイスの位置のトラッキング サービス (Device Location Tracking Services)]** > **[スイッチとアクセス ポイント (Switches and Access Points)]** を選択します。
 - ステップ 2 **[関連リンク (Related Links)]** から、**[非アクティブなスイッチおよびアクセス ポイント (Inactive Switches and Access Points)]** を選択し、**[移動 (Go)]** をクリックします。
[非アクティブなスイッチおよびアクセス ポイントの検索および表示 (Find and List Inactive Switches and Access Points)] ウィンドウに、トラッキングされていないインフラストラクチャ デバイスが表示されます。
 - ステップ 3 トラッキングを開始するスイッチまたはアクセス ポイントを選択します。
 - ステップ 4 **[選択項目の再アクティブ化 (Reactivate Selected)]** をクリックします。
-



第 **IV** 部

システムの管理

- システム ステータスのモニタ (107 ページ)
- アラーム (115 ページ)
- 監査ログ (137 ページ)
- Call Home (155 ページ)
- Serviceability Connector (169 ページ)
- 簡易ネットワーク管理プロトコル (175 ページ)
- サービス (225 ページ)
- Trace (265 ページ)
- 使用状況レコードの表示 (303 ページ)
- エンタープライズパラメータの管理 (311 ページ)
- サーバの管理 (315 ページ)



第 10 章

システムステータスのモニタ

- クラスタ ノード ステータスの表示 (107 ページ)
- ハードウェア ステータスの表示 (107 ページ)
- ネットワーク ステータスの表示 (108 ページ)
- インストールされているソフトウェアの表示 (108 ページ)
- システム ステータスの表示 (109 ページ)
- IP 設定の表示 (109 ページ)
- 最終ログインの詳細の表示 (110 ページ)
- ノードの ping (110 ページ)
- サービス パラメータの表示 (111 ページ)
- ネットワーク DNS の設定 (112 ページ)

クラスタ ノード ステータスの表示

この手順を使用して、クラスタ内のノードに関する情報を表示します。

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)] で、[表示 (Show)] > [クラスタ (Cluster)] を選択します。
 - ステップ 2** [クラスタ (Cluster)] ウィンドウのフィールドを調べます。フィールドの詳細については、オンラインヘルプを参照してください。
-

ハードウェア ステータスの表示

ハードウェア ステータスおよびシステム内のハードウェア リソースに関する情報を表示するには、この手順を実行します。

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)] で、[表示 (Show)]>[ハードウェア (Hardware)] を選択します。
- ステップ 2** [ハードウェア ステータス (Hardware Status)] ウィンドウのフィールドを調べます。フィールドの詳細については、オンラインヘルプを参照してください。
-

ネットワーク ステータスの表示

イーサネットおよび DNS 情報など、システムのネットワーク ステータスを表示するには、この手順を実行します。

表示されるネットワーク ステータス情報は、ネットワーク耐障害性が有効になっているかどうかによって異なります。

- ネットワーク耐障害性が有効になっていると、イーサネットポート 0 に障害が発生した場合、イーサネットポート 1 が自動的にネットワーク通信を管理します。
- ネットワーク耐障害性が有効になっている場合、ネットワークポートのイーサネット 0、イーサネット 1、および Bond 0 のネットワークステータス情報が表示されます。
- ネットワーク耐障害性が有効になっていない場合、イーサネット 0 のステータス情報のみが表示されます。

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)] で、[表示 (Show)]>[ネットワーク (Network)] を選択します。
- ステップ 2** [ネットワーク構成 (Network Configuration)] ウィンドウのフィールドを調べます。フィールドの詳細については、オンラインヘルプを参照してください。
-

インストールされているソフトウェアの表示

ソフトウェアのバージョンおよびインストールされているソフトウェアパッケージに関する情報を表示するには、この手順を実行します。

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)] で、[表示 (Show)]>[ソフトウェア (Software)] を選択します。

ステップ 2 [ソフトウェア パッケージ (Software Packages)] ウィンドウのフィールドを調べます。フィールドの詳細については、オンライン ヘルプを参照してください。

システム ステータスの表示

ロケール、稼働時間、CPU使用量、メモリ使用量などのシステム全体の状態を表示するには、この手順を実行します。

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)] で、[表示 (Show)] > [システム (System)] を選択します。

ステップ 2 [システム ステータス (System Status)] ウィンドウを調べます。フィールドの詳細については、オンライン ヘルプを参照してください。

IP 設定の表示

この手順を使用して、システムで利用可能な登録済みポートの一覧を表示します。

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)] で、[表示 (Show)] > [IP 設定 (IP Preferences)] を選択します。

ステップ 2 (任意) レコードをフィルタリングまたは検索するには、次のいずれかのタスクを実行します。

- 最初の一覧から検索パラメータを選択します。
- 2 番目の一覧から検索パターンを選択します。
- 必要に応じて、適切な検索テキストを指定します。

ステップ 3 [検索 (Find)] をクリックします。

ステップ 4 [システム ステータス (System Status)] ウィンドウに表示されるフィールドを調べます。フィールドの詳細については、オンライン ヘルプを参照してください。

最終ログインの詳細の表示

エンドユーザ（ローカルまたはLDAP クレデンシヤルを持つエンドユーザ）と管理者が Cisco Unified Communications Manager または IM and Presence Service の Web アプリケーションにログインすると、アプリケーションのメインウィンドウに、最後に成功したログインと最後に失敗したログインの詳細が表示されます。

SAML SSO 機能を使用してログインするユーザには、最後に成功したシステム ログイン情報だけが表示されます。ユーザが失敗した SAML SSO ログイン情報をトラッキングするには、ID プロバイダー（IdP）アプリケーションを参照できます。

次の Web アプリケーションには、ログイン試行に関する情報が表示されます。

- Cisco Unified Communications Manager:
 - Cisco Unified CM の管理
 - Cisco Unified のレポート
 - Cisco Unified サービスアビリティ
- IM and Presence Service
 - Cisco Unified CM IM and Presence の管理
 - Cisco Unified IM and Presence のレポート
 - Cisco Unified IM and Presence サービスアビリティ

Cisco Unified Communications Manager の次の Web アプリケーションでは、管理者だけがログインして最後のログイン詳細を表示できます。

- Disaster Recovery System
- Cisco Unified OS Administration

ノードの ping

ping ユーティリティを使用して、ネットワーク内の別のノードに ping します。この結果は、デバイスの接続の確認やトラブルシューティングに役立ちます。

手順

- ステップ 1 Cisco Unified Operating System Administration で、[サービス (Services)] > [Ping] を選択します。
- ステップ 2 [Ping の設定 (Ping Configuration)] ウィンドウで、各フィールドを設定します。フィールドとその設定オプションの詳細については、オンラインヘルプを参照してください。
- ステップ 3 [Ping] を選択します。

ping の結果が表示されます。

サービスパラメータの表示

クラスタ内のすべてのサーバで特定のサービスに属するサービスパラメータをすべて比較する必要がある場合があります。また、同期外れパラメータ（サーバ間で値が異なるサービスパラメータ）または提示された値から変更されているパラメータだけを表示する必要がある場合もあります。

次の手順を使用して、クラスタ内のすべてのサーバ上で特定のサービスに関するサービスパラメータを表示します。

手順

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

ステップ 2 [サーバ (Server)] ドロップダウンリストボックスで、サーバを選択します。

ステップ 3 [サービス (Service)] ドロップダウンリストボックスで、クラスタ内のすべてのサーバ上でサービスパラメータを表示するサービスを選択します。

(注) [サービスパラメータ設定 (Service Parameter Configuration)] ウィンドウに、すべてのサービス（アクティブと非アクティブ）が表示されます。

ステップ 4 表示された [サービスパラメータ設定 (Service Parameter Configuration)] ウィンドウの [関連リンク (Related Links)] ドロップダウンリストボックスで [すべてのサーバに対するパラメータ (Parameters for All Servers)] を選択してから、[移動 (Go)] をクリックします。

[すべてのサーバに対するパラメータ (Parameters for All Servers)] ウィンドウが表示されます。現在のサービスに関して、すべてのパラメータがアルファベット順に一覧表示されます。パラメータごとに、推奨値がパラメータ名の横に表示されます。各パラメータ名の下に、そのパラメータを含むサーバのリストが表示されます。各サーバ名の横に、このサーバのパラメータの現在値が表示されます。

特定のパラメータについて、対応するサービスパラメータ ウィンドウにリンクするサーバ名または現在のパラメータ値をクリックし、その値を変更します。[前へ (Previous)] と [次へ (Next)] をクリックすると、[すべてのサーバに対するパラメータ (Parameters for All Servers)] ウィンドウ間を移動できます。

ステップ 5 同期外れサービスパラメータを表示する必要がある場合は、[関連リンク (Related Links)] ドロップダウンリストボックスで、[すべてのサーバに対する同期外れパラメータ (Out of Sync Parameters for All Servers)] を選択してから、[移動 (Go)] をクリックします。

[すべてのサーバに対する同期外れパラメータ (Out of Sync Parameters for All Servers)] ウィンドウが表示されます。現在のサービスに関して、サーバごとに値が異なるサービスパラメータがアルファベット順に表示されます。パラメータごとに、推奨値がパラメータ名の横に表示さ

れます。各パラメータ名の下に、そのパラメータを含むサーバのリストが表示されます。各サーバ名の横に、このサーバのパラメータの現在値が表示されます。

特定のパラメータについて、対応するサービスパラメータウィンドウにリンクするサーバ名または現在のパラメータ値をクリックして、その値を変更します。[前へ (Previous)] と [次へ (Next)] をクリックすると、[すべてのサーバに対する同期外れパラメータ (Out of Sync Parameters for All Servers)] ウィンドウ間を移動できます。

- ステップ 6** 推奨値から変更されたサービスパラメータを表示する必要がある場合は、[関連リンク (Related Links)] ドロップダウン リスト ボックスで、[すべてのサーバに対する変更済みパラメータ (Modified Parameters for All Servers)] を選択してから、[移動 (Go)] をクリックします。

[すべてのサーバに対する変更済みパラメータ (Modified Parameters for All Servers)] ウィンドウが表示されます。現在のサービスに関して、推奨値とは異なる値を持つサービスパラメータがアルファベット順に表示されます。パラメータごとに、推奨値がパラメータ名の横に表示されます。各パラメータ名の下に、推奨値とは異なる値を持つサーバのリストが表示されます。各サーバ名の横に、このサーバのパラメータの現在値が表示されます。

特定のパラメータについて、対応するサービスパラメータウィンドウにリンクするサーバ名または現在のパラメータ値をクリックして、その値を変更します。[前へ (Previous)] と [次へ (Next)] をクリックすると、[すべてのサーバに対する変更済みパラメータ (Modified Parameters for All Servers)] ウィンドウ間を移動できます。

ネットワーク DNS の設定

DNS ネットワークを設定するには、この手順を使用します



- (注) Cisco Unified CM Administration で、DHCP 設定ウィンドウによって DNS プライマリおよびセカンダリ サーバを割り当てることもできます。

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** DNS サーバを割り当てる場合は、パブリッシュャ ノードに次の commandson のいずれかを実行します。
- プライマリ DNS サーバを割り当てるには、**set network dns primary <ip_address>** を実行します
 - セカンダリ DNS サーバを割り当てるには、**set network dns secondary <ip_address>** を実行します

ステップ 3 追加の DNS オプションを割り当てるには、**set network dns options [timeout| seconds] [attempts| number] [rotate]** を実行します。

- **timeout** で DNS タイムアウトを設定します
- **second** はタイムアウトの秒数です
- **attempt** は DNS 要求の試行回数を設定します
- **number** は試行回数を指定します
- **rotate** を指定すると、設定されている DNS サーバのローテーションが行われ、負荷が分散されます

たとえば、**set network dns options timeout 60 attempts 4 rotate** などとします
サーバは、このコマンドの実行後に再起動します。



第 11 章

アラーム

- [概要 \(115 ページ\)](#)
- [アラーム設定 \(116 ページ\)](#)
- [アラームの定義 \(117 ページ\)](#)
- [アラーム情報 \(118 ページ\)](#)
- [アラームのセットアップ \(119 ページ\)](#)
- [アラーム サービスの設定 \(120 ページ\)](#)
- [アラーム定義およびユーザ定義の説明の追加 \(129 ページ\)](#)

概要

Cisco Unified Serviceability、Cisco Unified IM and Presence のサービスアビリティアラームは、実行時のステータスとシステムの状態に関する情報を提供するため、システムに関する問題を修復できます。たとえば、ディザスタリカバリシステムを使用して問題を特定します。説明と推奨処置を含むアラーム情報には、トラブルシューティングを支援し、クラスタにも適用するために、アプリケーション名、マシン名なども含まれています。

アラーム情報を複数の場所に送信するようにアラームインターフェイスを設定し、それぞれの場所に独自のアラームイベントレベル（デバッグから緊急まで）を持たせることができます。Syslog ビューア（ローカル syslog）、Syslog ファイル（リモート syslog）、SDL トレース ログファイル（Cisco CallManager、CTIManager サービスのみ）、またはすべての宛先にアラームを送信できます。

サービスがアラームを発行すると、アラームインターフェイスはユーザが設定し、アラーム定義のルーティングリストに指定されている場所（たとえば、SDI トレース）にアラーム情報を送信します。システムは、SNMP トラップと同様にアラーム情報を転送することや、アラーム情報を最終宛先に書き込むことができます（ログファイルなど）。

Cisco Database Layer Monitor などのサービスのアラームを特定のノードで設定したり、クラスタのすべてのノードで特定のサービスのアラームを設定することができます。



(注) Cisco Unity Connection の SNMP ではトラップをサポートしていません。



ヒント リモート Syslog サーバの場合は、Cisco Unified Communications Manager サーバを指定しないでください。このサーバは他のサーバからの Syslog メッセージを受け入れることができません。

Cisco Unified Real-Time Monitoring Tool (Unified RTMT) の Trace and Log Central オプションを使用して、SDL トレース ログ ファイルに送信されるアラームを収集します (Cisco CallManager、CTI Manager サービスの場合のみ)。ローカル Syslog に送信されるアラーム情報を表示するには、Unified RTMT で Syslog ビューアを使用します。

アラーム設定

シスコの統合型の有用性で、Cisco Database Layer Monitor などのサービスのアラームを設定できます。その後、システムがアラーム情報を送信する、Syslog ビューア (ローカル syslog) などのロケーションを設定します。このオプションを使用すると、次の操作を実行できます。

- 特定のサーバまたはすべてのサーバ (Unified Communications Manager クラスタのみ) のサービスにアラームを設定する
- 設定済みのサービスまたはサーバに異なるリモート syslog サーバを設定する
- 異なる宛先に異なるアラーム イベント レベルを設定する

Cisco Unified Communications Manager Administration の Cisco Syslog Agent エンタープライズ パラメータによって、リモート syslog サーバ名と syslog シビラティ (重大度) の 2 つの設定を使用して、設定されたしきい値を満たしているか、または超えているすべてのアラームをリモート syslog サーバに転送できます。これらの Cisco Syslog Agent のパラメータにアクセスするには、使用している構成に対応する次のウィンドウを開きます。

Unified Communications Manager	Cisco Unified Communications Manager Administration で、[システム (System)] > [エンタープライズ パラメータ (Enterprise Parameters)] を選択します。
Cisco Unity Connection	Cisco Unity Connection Administration で、[システム設定 (System Setting)] > [エンタープライズ パラメータ (Enterprise Parameters)] を選択します。
Cisco IM and Presence	Cisco Unified Communications Manager IM and Presence Administration で、[システム (System)] > [エンタープライズ パラメータ (Enterprise Parameters)] を選択します。

このアラームには、システム (OS/ハードウェアプラットフォーム)、アプリケーション (サービス)、およびセキュリティの各アラームが含まれます。



(注) Cisco Syslog Agent アラーム エンタープライズ パラメータとアプリケーション (サービス) アラームの両方を Cisco Unified Serviceability で設定すると、リモートの syslog に同じアラームが 2 回送信されることがある。

ローカル syslog がアプリケーションアラームに対して有効になっている場合、ローカルの syslog しきい値とエンタープライズしきい値の両方をアラームが超えたときにだけ、エンタープライズリモート syslog サーバにアラームが送信される。

Cisco Unified Serviceability でリモートの syslog も有効になっている場合、システムは、Cisco Unified Serviceability で設定されているアプリケーションしきい値を使用してリモート syslog サーバにアラームを転送します。このため、リモート syslog サーバにアラームが 2 回送信される場合があります。

イベント レベル/シビラティ (重大度) 設定は、システムが収集するアラームおよびメッセージにフィルタリングメカニズムを提供します。この設定は、Syslog およびトレースファイルが過負荷状態になるのを防ぎます。設定されたしきい値を超えるアラームおよびメッセージのみが転送されます。

アラームおよびイベントに関連するシビラティ (重大度) レベルの詳細については、[アラームの定義 \(117 ページ\)](#) を参照してください。

アラームの定義

アラーム定義とは、参照用に使用され、アラームの意味やアラームからの回復方法など、アラームメッセージについて説明するものです。アラーム情報は、[アラーム定義 (Alarm Definitions)] ウィンドウで参照します。サービス固有のアラーム定義をクリックすると、アラーム情報に関する説明 (追加したユーザ定義のテキストなど) と推奨されるアクションが表示されます。

Serviceability GUI で表示されるすべてのアラームのアラーム定義を検索できます。問題のトラブルシューティングを支援するため、対応するカタログに存在する定義には、アラーム名、記述、説明、推奨されるアクション、シビラティ (重大度)、パラメータ、モニタなどが含まれています。

システムでアラームが生成されると、アラーム情報内のアラーム定義の名前が使用されるため、アラームを識別できます。アラーム定義では、システムがアラーム情報を送信できる場所が指定されたルーティングリストを表示できます。ルーティングリストには、次の場所が含まれます。これは、[アラーム設定 (Alarm Configuration)] ウィンドウで設定できる場所に対応します。

- Unified Communications Manager のみ : [SDL] : アラームでこのオプションをイネーブルにし、[アラーム設定 (Alarm Configuration)] ウィンドウでイベントレベルを指定した場合、アラーム情報は SDL トレースに送られます。

- [SDI] : アラームでこのオプションをイネーブルにし、[アラーム設定 (Alarm Configuration)] ウィンドウでイベント レベルを指定した場合、アラーム情報は SDI トレースに送られます。
- [システムログ (Sys Log)] : アラームでこのオプションをイネーブルにし、[アラーム設定 (Alarm Configuration)] ウィンドウでイベント レベルを指定して、リモート Syslog サーバのサーバ名または IP アドレスを入力した場合、アラーム情報はリモート Syslog サーバに送られます。
- [イベントログ (Event Log)] : アラームでこのオプションをイネーブルにし、[アラーム設定 (Alarm Configuration)] ウィンドウでイベント レベルを指定した場合、アラーム情報はローカル Syslog に送られます。この情報は Cisco Unified Real-Time Monitoring Tool (Unified RTMT) の SysLog ビューアで表示できます。
- [データコレクタ (Data Collector)] : アラーム情報はリアルタイム情報システム (RIS データコレクタ) に送られます (アラート目的のみ)。このオプションは [アラーム設定 (Alarm Configuration)] ウィンドウで設定できません。
- [SNMP トラップ (SNMP Traps)] : SNMP トラップが生成されます。このオプションは [アラーム設定 (Alarm Configuration)] ウィンドウで設定できません。



ヒント SNMP トラップの場所がルーティング リストに表示されている場合、アラーム情報が CCM MIB SNMP エージェントに送られ、CISCO-CCM-MIB 内の定義に従ってトラップが生成されます。

[アラーム設定 (Alarm Configuration)] ウィンドウで特定の場所に対して設定されたアラーム イベントレベルが、アラーム定義に設定されているシビラティ (重大度) 以下の場合、システムはアラームを送信します。たとえば、アラーム定義のシビラティ (重大度) が WARNING_ALARM で、[アラーム設定 (Alarm Configuration)] ウィンドウで特定の宛先のアラーム イベントレベルをそれよりも低い「警告」、「通知」、「情報」、または「デバッグ」として設定した場合、アラームは対応する宛先に送られます。アラーム イベントレベルを「緊急」、「アラート」、「重要」、または「エラー」として設定した場合、アラームは対応する場所に送られません。

各アラーム定義について、追加説明または推奨事項を含めることができます。すべての管理者が追加情報にアクセスできます。[アラームの詳細 (Alarm Details)] ウィンドウに表示される [ユーザ定義テキスト (User Defined Text)] ペインに直接情報を入力します。標準的な水平および垂直スクロールバーでスクロールできます。Cisco Unified Serviceability により、データベースに情報が追加されます。

アラーム情報

アラーム情報を表示して、問題が存在するかどうかを特定できます。アラーム情報を表示するために使用する方法は、アラームを設定するときに選択した宛先に依存します。SDL トレース ログファイル (Unified Communications Manager) に送信されるアラーム情報を表示するには、

Unified RTMT の Trace and Log Central オプションを使用するか、テキストエディタを使用します。ローカル syslog に送信されるアラーム情報を表示するには、Unified RTMT の SysLog ビューアを使用します。

アラームのセットアップ

アラームをセットアップするには、次の手順を実行します。

手順

- ステップ 1** Cisco Unified Communications Manager Administration、Cisco Unity Connection Administration または Cisco Unified IM and Presence Administration で、指定したリモート Syslog サーバにシステム、アプリケーション（サービス）、およびセキュリティのアラーム/メッセージを送信するように Cisco Syslog Agent エンタープライズ パラメータを設定します。Cisco Unified Serviceability でアプリケーション（サービス）アラーム/メッセージを設定する場合は、この手順をスキップしてください。
 - ステップ 2** Cisco Unified Serviceability では、収集するアプリケーション（サービス）アラーム情報のサーバ、サービス、宛先、およびイベント レベルを設定します。
 - ステップ 3** （任意）アラームに定義を追加します。
 - サービスはすべて SDI ログに出力できます（ただし、トレースでも設定する必要があります）。
 - すべてのサービスは SysLog ビューアに出力できます。
 - Unified Communications Manager のみ：Cisco CallManager サービスと Cisco CTIManager サービスでのみ、SDL ログを使用します。
 - Syslog メッセージをリモート Syslog サーバに送信するには、宛先として [リモート Syslog (Remote Syslog)] チェック ボックスをオンにし、ホスト名を指定します。リモートサーバ名を設定していない場合、Cisco Unified Serviceability はリモート Syslog サーバに Syslog メッセージを送信しません。
- ヒント** Unified Communications Manager サーバをリモート Syslog サーバとして設定しないでください。
- ステップ 4** アラームの宛先として SDL トレース ファイルを選択した場合は、Unified RTMT の Trace and Log Central オプションを使用してトレースの収集と情報の表示を行います。
 - ステップ 5** アラームの宛先としてローカル Syslog を選択した場合は、Unified RTMT の SysLog ビューアでアラーム情報を表示します。
 - ステップ 6** 説明と推奨されるアクションについては、対応するアラーム定義を参照してください。

アラーム サービスの設定

Syslog Agent エンタープライズ パラメータ

Cisco Syslog Agent エンタープライズパラメータは、設定されたしきい値を超過したシステム、アプリケーション、セキュリティアラームまたはメッセージを指定したリモート syslog サーバに送信するように設定できます。Cisco Syslog Agent のパラメータにアクセスするには、使用している構成に対応する次のウィンドウを開きます。

Unified Communications Manager	Cisco Unified Communications Manager Administration で、[システム (System)] > [エンタープライズ パラメータ (Enterprise Parameters)] を選択します。
Cisco Unity Connection	Cisco Unity Connection Administration で、[システム設定 (System Setting)] > [エンタープライズ パラメータ (Enterprise Parameters)] を選択します。
Cisco IM and Presence	Cisco Unified Communications Manager IM and Presence Administration で、[システム (System)] > [エンタープライズ パラメータ (Enterprise Parameters)] を選択します。

次に、リモート syslog サーバ名 (リモート Syslog サーバ名1、リモート syslog サーバ名2、リモート Syslog サーバ名3、リモート Syslog サーバ名4、およびリモート Syslog サーバ名 5) と syslog のシビラティ (重大度) を設定します。サーバ名を設定するときに、有効な IP アドレスを指定していることを確認します。Syslog のシビラティ (重大度) は、設定したすべてのリモート syslog サーバに適用されます。次に [保存 (Save)] をクリックします。[?] ボタンをクリックすると、入力できる有効な値が表示されます。サーバ名が指定されていないと、Cisco Unified Serviceability は Syslog メッセージを送信しません。



注意 Unified Communications Manager でリモート syslog サーバを設定する際は、リモート syslog サーバ名に重複するエントリを追加しないでください。重複するエントリを追加した場合、Cisco Syslog Agent はメッセージをリモート syslog サーバに送信するときに重複したエントリを無視します。



(注) Unified Communications Manager をリモート Syslog サーバとして設定しないでください。Unified Communications Manager ノードは、別のサーバからの Syslog メッセージを受け入れません。

アラームサービスのセットアップ

ここでは、Cisco Unified Serviceability で管理する機能サービスやネットワーク サービスのアラームを追加または更新する方法について説明します。



(注) SNMP トラップとカタログの設定は変更しないことを推奨します。

Cisco Unity Connection では、Cisco Unity Connection Serviceability で使用可能なアラームも使用します。Cisco Unity Connection Serviceability ではアラームを設定できません。詳細については、『Cisco Unity Connection Serviceability アドミニストレーションガイド』を参照してください。標準のレジストリ エディタの使用方法の詳細については、使用している OS のオンラインドキュメントを参照してください。

手順

ステップ 1 [アラーム (Alarm)] > [設定 (Configuration)] を選択します。

[アラーム設定 (Alarm Configuration)] ウィンドウが表示されます。

ステップ 2 [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を選択し、[移動 (Go)] をクリックします。

ステップ 3 [サービスグループ (Service Group)] ドロップダウン リストから、アラームを設定するサービスのカテゴリ ([データベースおよび管理サービス (Database and Admin Services)] など) を選択し、[移動 (Go)] をクリックします。

ヒント サービスグループに対応するサービスの一覧については、「サービスグループ」を参照してください。

ステップ 4 [サービス (Service)] ドロップダウン リストからアラームを設定するサービスを選択し、[移動 (Go)] をクリックします。

サービスグループと設定をサポートするサービスだけが表示されます。

ヒント ドロップダウン リストには、アクティブなサービスと非アクティブのサービスが表示されます。

[アラーム設定 (Alarm Configuration)] ウィンドウで、選択したサービスのイベントレベルが表示されたアラームモニタのリストが表示されます。また、[すべてのノードに適用 (Apply to All Nodes)] チェックボックスも表示されます。

ステップ 5 Unified Communications Manager のみ：クラスタをサポートしている設定の場合は、必要に応じて [すべてのノードに適用 (Apply to All Nodes)] チェックボックスをオンにして、クラスタ内のすべてのノードにサービスのアラーム設定を適用することができます。

ステップ 6 「アラーム設定」の説明に従って設定を行います。この項ではモニタおよびイベントレベルについても説明されています。

ステップ 7 設定を保存するには、[保存 (Save)] ボタンをクリックします。

(注) デフォルトを設定するには、[デフォルトの設定 (Set Default)] ボタンをクリックしてから、[保存 (Save)] をクリックします。

次のタスク



ヒント [アラーム設定 (Alarm Configuration)] ウィンドウで特定の宛先に対して設定されたアラーム イベントレベルが、アラーム定義に設定されているシビラティ (重大度) 以下の場合、アラームが送信されます。たとえば、アラーム定義のシビラティ (重大度) が `WARNING_ALARM` で、[アラーム設定 (Alarm Configuration)] ウィンドウで特定の宛先のアラーム イベントレベルをそれよりも低い「警告」、「通知」、「情報」、または「デバッグ」として設定した場合、アラームは対応する宛先に送られます。アラーム イベントレベルを、シビラティ (重大度) がより高い「緊急」、「警報」、「重大」、または「エラー」として設定した場合、アラームは対応する場所に送られません。

Cisco エクステンション モビリティ アプリケーション サービス、Cisco Unified Communications Manager Assistant サービス、Cisco エクステンション モビリティ サービス、および Cisco WebDialer サービスのアラーム定義にアクセスするには、「アラーム定義」で説明されている [アラームメッセージ定義 (Alarm Messages Definitions)] ウィンドウの [JavaApplications] カテゴリを選択します。

Cisco Tomcat を使用するアラーム サービスのセットアップ

次のサービスは、アラームの生成に Cisco Tomcat を使用します。

- Cisco Extension Mobility アプリケーション
- Cisco IP Manager Assistant
- Cisco エクステンション モビリティ
- Cisco Web Dialer

システム ログイン アラーム AuthenticationFailed も Cisco Tomcat を使用します。これらのサービスに対してアラームを生成するには、次の手順を実行します。

手順

ステップ 1 Cisco Unified Serviceability で、[アラーム (Alarm)] > [設定 (Configuration)] 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、アラームを設定するサーバを選択し、[移動 (Go)] をクリックします。

- ステップ 3** [サービスグループ (Services Group)] ドロップダウンリストから、[プラットフォームサービス (Platform Services)] を選択し、[移動 (Go)] をクリックします。
- ステップ 4** [サービス (Services)] ドロップダウンリストから、[CiscoTomcat] を選択し、[移動 (Go)] をクリックします。
- ステップ 5** Unified Communications Manager のみ：クラスタをサポートしている設定の場合は、必要に応じて [すべてのノードに適用 (Apply to All Nodes)] チェックボックスをオンにして、クラスタ内のすべてのノードにサービスのアラーム設定を適用できます。
- ステップ 6** 「アラーム設定」の説明に従って設定を行います。この項ではモニタおよびイベントレベルについても説明されています。
- ステップ 7** 設定を保存するには、[保存 (Save)] ボタンをクリックします。

サービスグループ

次の表に、[アラーム設定 (Alarm Configuration)] ウィンドウの [サービスグループ (Service Group)] ドロップダウンリストボックスに表示されるオプションに対応するサービスの一覧を示します。

(注) 一覧されているすべてのサービスグループとサービスが、すべてのシステム設定に適用されるわけではありません。

表 7: アラーム設定のサービスグループ

サービスグループ	サービス
CM サービス (CM Services)	Cisco CTIManager、Cisco CallManager、Cisco DHCP Monitor サービス、Cisco Dialed Number Analyzer、Cisco Dialed Number Analyzer Server、Cisco Extended Functions、Cisco IP Voice Media Streaming App、Cisco Messaging Interface、Cisco Headset サービス、および Cisco TFTP
CTI サービス	Cisco IP Manager Assistant および Cisco WebDialer Web サービス
CDR サービス	Cisco CAR Scheduler、Cisco CDR Agent、および Cisco CDR Repository Manager
データベースおよび管理者サービス	Cisco Bulk Provisioning Service と Cisco Database Layer Monitor
パフォーマンスおよびモニタリングサービス (Performance and Monitoring Services)	Cisco AMC サービスおよび Cisco RIS Data Collector

サービスグループ	サービス
ディレクトリサービス	Cisco DirSync
バックアップおよび復元サービス	Cisco DRF Local および Cisco DRF Master
System Services	Cisco Trace Collection Service
プラットフォームサービス	Cisco Tomcat と Cisco Smart License Manager

アラーム設定

次の表で、すべてのアラームの構成時の設定について説明します。サービスでこれらの設定をサポートしていない場合もあります。

表 8: アラーム設定

名前	説明
[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。
サービスグループ	<p>Cisco Unity Connection がサポートしているサービス グループは、[データベースおよび管理サービス (Database and Admin Services)]、[パフォーマンスおよびモニタリング サービス (Performance and Monitoring Services)]、[バックアップおよび復元サービス (Backup and Restore Services)]、[システムサービス (System Services)]、[プラットフォーム サービス (Platform Services)] だけです。</p> <p>ドロップダウンリストからアラームを設定するサービスのカテゴリ ([データベースおよび管理サービス (Database and Admin Services)] など) を選択し、[移動 (Go)] をクリックします。</p>

名前	説明
サービス	<p>[サービス (Service)] ドロップダウンリストからアラームを設定するサービスを選択し、[移動 (Go)] をクリックします。</p> <p>サービスグループと設定をサポートするサービスだけが表示されます。</p> <p>ヒント ドロップダウンリストには、実行中のサービスと実行されていないサービスの両方が表示されます。</p>
Unified Communications Manager および Cisco Unified Communications Manager IM and Presence Serviceのみ： すべてのノードに適用 (Apply to All Nodes)	<p>クラスタ内のすべてのノードにサービスのアラーム設定を適用するには、このチェックボックスをオンにします。</p>
ローカル Syslog のアラームの イネーブル化 (Enable Alarm for Local Syslogs)	<p>SysLog ビューアがアラームの宛先として機能します。プログラムはエラーを Syslog ビューアの [アプリケーション ログ (Application Logs)] に記録して、アラームの説明と推奨処置を提供します。Syslog ビューアには Cisco Unified Real-Time Monitoring Tool からアクセスできます。</p> <p>Syslog ビューアでのログの表示については、『Cisco Unified Real-Time Monitoring Tool Administration Guide』を参照してください。</p>

名前	説明
リモート Syslog のアラームのイネーブル化 (Enable Alarm for Remote Syslogs)	<p>SysLog ファイルがアラームの宛先として機能します。このチェックボックスをオンにすると、Syslog メッセージを Syslog サーバに保存して、その Syslog サーバの名前を指定することができます。この宛先が有効になっているときにサーバ名が指定されていないと、Cisco Unified Serviceability は Syslog メッセージを送信しません。</p> <p>設定されている AMC プライマリとフェールオーバー コレクタは、リモート Syslog 設定を使用します。コレクタが使用するリモート Syslog 設定は、個々のノードでそれぞれ設定されている設定です。</p> <p>リモート Syslog が AMC プライマリ コレクタでのみ設定されていて、AMC フェールオーバー コレクタでリモート Syslog が設定されていないときに、AMC プライマリ コレクタでフェールオーバーが発生すると、リモート Syslog は生成されません。</p> <p>すべてのノードで同じ設定を正確に行い、リモート Syslog アラームが同じリモート Syslog サーバに送信されるようにする必要があります。</p> <p>フェールオーバーが AMC コントローラで発生した場合、またはコレクタの設定が別のノードに変更される場合は、バックアップ ノードまたは新たに設定されたノードのリモート Syslog の設定が使用されます。</p> <p>システムで非常に多くのアラームがフラッディングするのを防ぐには、[エンドポイントアラームを除外 (Exclude End Point Alarms)] チェックボックスをオンにします。これにより、エンドポイントの電話関連のイベントが別のファイルに記録されるようになります。</p> <p>[エンドポイントアラームを除外 (Exclude End Point Alarms)] チェックボックスは Call Manager サービスの場合にのみ表示され、デフォルトでは選択されていません。このチェックボックスをオンにする場合は、[すべてのノードに適用 (Apply to All Nodes)] もオンにする必要があります。エンドポイントアラームの設定オプションは、[アラームの設定 (Alarm configuration settings)] に表示されます。</p> <p>ヒント ノードは他のノードからの Syslog メッセージを受け付けられないため、Unified Communications Manager あるいは Cisco Unified Communications Manager IM and Presence Service ノードを通知先として指定しないでください。</p>

名前	説明
リモート Syslog サーバ (Remote Syslog Server)	<p>[サーバ名 1 (Server Name 1)]、[サーバ名 2 (Server Name 2)]、[サーバ名 3 (Server Name 3)]、[サーバ名 4 (Server Name 4)]、[サーバ名 5 (Server Name 5)]の各フィールドに、Syslog メッセージを受け入れるために使用するリモート Syslog サーバの名前または IP アドレスを入力します。たとえば、アラームを Cisco Unified Operations Manager に送信する場合は、Cisco Unified Operations Manager をサーバ名として指定します。</p> <p>ヒント ノードは他のノードからの Syslog メッセージを受け付けられないため、Unified Communications Manager あるいは Cisco Unified Communications Manager IM and Presence Service ノードを通知先として指定しないでください。</p>
SDI トレースのアラームのイネーブル化 (Enable Alarm for SDI Trace)	<p>SDI トレースライブラリがアラームの宛先として機能します。アラームを記録するには、このチェックボックスをオンにして、選択されたサービスの [トレース設定 (Trace Configuration)] ウィンドウで [トレース オン (Trace On)] チェックボックスをオンにします。Cisco Unified Serviceability の [トレース設定 (Trace Configuration)] ウィンドウの構成時の設定の詳細については、トレース パラメータのセットアップを確認します。</p>
Unified Communications Manager および Unified Communications Manager BE のみ : SDL トレースのアラームのイネーブル化 (Enable Alarm for SDL Trace)	<p>SDL トレース ライブラリがアラームの宛先として機能します。この宛先は Cisco CallManager サービスと CTIManager サービスの場合にのみ使用できます。このアラームの宛先を設定するには、Trace SDL の設定を使用します。SDL トレース ログ ファイルにアラームのログを記録するには、このチェックボックスをオンにして、選択したサービスの [トレース設定 (Trace Configuration)] ウィンドウで [トレース オン (Trace On)] チェックボックスをオンにします。Cisco Unified Serviceability の [トレース設定 (Trace Configuration)] ウィンドウの構成時の設定の詳細については、トレース パラメータのセットアップを確認します。</p>

名前	説明
Alarm Event Level	<p>ドロップダウン リストから、次のオプションのいずれかを選択します。</p> <p>緊急 このレベルは、システムを使用不能と指定します。</p> <p>アラート このレベルは、ただちに対処が必要であることを示します。</p> <p>重大 システムがクリティカルな状態を検出します。</p> <p>エラー このレベルは、エラーがあることを示します。</p> <p>警告 このレベルは、警告状態が検出されたことを示します。</p> <p>注記 このレベルは、正常ではあるものの重要な状態を示します。</p> <p>情報 このレベルは、情報メッセージだけを示します。</p> <p>デバッグ このレベルは、Cisco Technical Assistance Center のエンジニアがデバッグに使用する詳細イベント情報を示します。</p>

次の表に、デフォルトのアラームの構成時の設定について説明します。

	ローカル syslog	リモート syslog	SDI トレース	SDL トレース
Enable Alarm	オン	オフ	オン	オン
Alarm Event Level	Error	無効	Error	Error

エンドポイントアラームを除外	ローカル Syslog	代替 syslog	リモート Syslog	Syslog のシビラティ (重大度) とアラートの絞り込み	Syslog トラップ
オン	いいえ	はい	いいえ	いいえ	いいえ
オフ	いいえ	はい	はい	はい	はい

アラーム定義およびユーザ定義の説明の追加

ここでは、Serviceability のインターフェイスに表示されるアラーム定義のユーザ情報を検索、表示、作成する手順について説明します。

アラーム定義の表示とユーザ定義の説明の追加

ここでは、アラーム定義を検索して表示する方法について説明します。



ヒント Unified Communications Manager および Cisco Unity Connection のみ：Cisco Unity Connection Serviceability で Cisco Unity Connection アラーム定義を表示することができます。Cisco Unity Connection Serviceability ではアラーム定義にユーザ定義の説明を追加できません。

また、Cisco Unity Connectionは、シスコユニファイドサービスの特定のアラーム定義も使用します。シスコのユニファイドサービスでは、これらの定義を確認する必要があります。システムカタログのカタログに関連付けられているアラームが表示可能であることに注意してください。

始める前に

アラーム定義カタログの記述を確認してください。

手順

ステップ 1 [アラーム (Alarm)] > [定義 (Definitions)] を選択します。

ステップ 2 次のいずれかの操作を実行します。

- 次のようにアラームを選択します。
 - [アラームの検索場所 (Find alarms where)] ドロップダウンリストからアラーム カタログを選択します。たとえば、システムアラーム カタログまたは IM and Presence アラーム カタログを選択します。
 - [等しい (Equals)] ドロップダウンリストから特定のカタログ名を選択します。
- [アラーム名を入力 (Enter Alarm Name)] フィールドにアラーム名を入力します。

ステップ 3 [検索] を選択します。

ステップ 4 複数のアラーム定義ページが存在する場合は、次のいずれかの操作を実行します。

- 別のページを選択するには、[アラームメッセージ定義 (Alarm Message Definitions)] ウィンドウで適切なナビゲーション ボタンを選択します。

- ウィンドウに表示されるアラームの数を変更するには、[ページあたりの行数 (Rows Per Page)] ドロップダウンリストから別の値を選択します。

ステップ 5 アラームの詳細を設定するアラーム定義を選択します。

ステップ 6 アラームに情報を追加する場合は、[ユーザ定義テキスト (User Defined Text)] フィールドにテキストを入力し、[保存 (Save)] を選択します。

ヒント [ユーザ定義テキスト (User Defined Text)] フィールドにテキストを追加する場合、いつでも [すべてクリア (Clear All)] を選択して入力した情報を削除できます。

ステップ 7 [保存] を選択します。

ステップ 8 [アラーム メッセージ定義 (Alarm Message Definitions)] ウィンドウに戻るには、[関連リンク (Related Links)] ドロップダウンリストから [アラームの検索/リストに戻る (Back to Find/List Alarms)] を選択します。

ステップ 9 [移動 (Go)] を選択します。

システムアラームカタログの説明

次の表に、システムアラームカタログのアラームの説明を示します。システムアラームカタログでは、Cisco Unified Communications Manager および Cisco Unity Connection をサポートしています。

表 9: システム カタログ

名前	説明
ClusterManagerAlarmCatalog	クラスタ内のサーバ間のセキュリティアソシエーションの確立にすべての Cluster Manager アラーム定義。
DBAlarmCatalog	すべてのシスコ データベース アラーム定義
DRFAlarmCatalog	すべてのディザスタリカバリ システム アラーム定義
GenericAlarmCatalog	すべてのアプリケーションで共有されるすべての汎用アラーム定義
JavaApplications	すべての Java アプリケーション アラーム定義。 ヒント アラーム設定 GUI を使用して JavaApplications アラームを定義することはできません。Unified Communications Manager および Unity Connection の場合は、通常はこれらのアラームをアラームカタログに送るよう設定します。Unified Communications Manager の場合は、これらのアラームは SNMP トラップを生成して LAN Management Solution と統合するように設定します。アラーム定義とパラメータを表示および変更するには、オペレーション システムに付属しているレジストリエディタを使用します。

名前	説明
EMAlarmCatalog	エクステンション モビリティのアラーム
LoginAlarmCatalog	すべてのログイン関連のアラーム定義
LpmTctCatalog	すべてのログパーティションモニタリングおよびトレース収
RTMTAlarmCatalog	すべての Cisco Unified Real-Time Monitoring Tool アラーム定義
SystemAccessCatalog	SystemAccess がすべてのプロセス統計カウンタと共にすべての カウンタを提供するかどうかのトラッキングに使用されるす 定義。
ServiceManagerAlarmCatalogs	サービスのアクティブ化、非アクティブ化、開始、リスター に関連するすべての Service Manager アラーム定義。
TFTPAlarmCatalog	すべての Cisco TFTP アラーム定義
TVSAlarmCatalog	信頼検証サービスのアラーム
TestAlarmCatalog	コマンドライン インターフェイス (CLI) から SNMP トラッ トアラームを送信するために使用されるすべてのアラーム定 については、『Cisco Unified Solutions コマンドライン インター ファレンス ガイド』を参照してください。 ヒント Cisco Unity ConnectionSNMP は、Unified Communic と Cisco Unity Connection システムのいずれかでトラ トしていません。
CertMonitorAlarmCatalog	すべての証明書の有効期限の定義。
CTLproviderAlarmCatalog	Certificate Trust List (CTL) Provider サービスのアラーム
CDPAlarmCatalog	Cisco Discovery Protocol (CDP) サービスのアラーム
IMSAlarmCatalog	すべてのユーザ認証とクレデンシャルの定義。
SLMAlarmCatalog	シスコ スマート ライセンシングのアラーム

CallManager アラーム カタログの説明

ここで説明する内容は、Cisco Unity Connection には適用されません。

次の表に、CallManager アラームカタログの説明を示します。

表 10: CallManager アラーム カタログ

名前	説明
CallManager	すべての Cisco CallManager サービスのアラーム定義
CDRRepAlarmCatalog	すべての CDRRep アラーム定義
CARAlarmCatalog	すべての CDR 分析とレポート アラーム定義
CEFAAlarmCatalog	すべての Cisco Extended Functions アラーム定義
CMIAAlarmCatalog	すべての Cisco Messaging Interface のアラーム定義
CtiManagerAlarmCatalog	すべての Cisco Computer Telephony Integration (CTI) マネージャの定義
IpVmsAlarmCatalog	すべての IP Voice Media Streaming Application のアラーム定義
TCDSRVAAlarmCatalog	すべての Cisco Telephony Call Dispatcher サービスのアラーム定義
電話	ダウンロードなどの電話関連タスクに対するアラーム
CAPFAlarmCatalog	Certificate Authority Proxy Function (CAPF) サービスに対するアラーム
SAMLSSOAlarmCatalog	SAML シングルサインオン機能のアラーム。

IM and Presence アラーム カタログの説明

次の表に、IM and Presence Service アラーム カタログの説明を示します。

表 11: IM and Presence Service アラーム カタログ

名前	説明
CiscoUPSConfigAgent	IM and Presence Service IDS データベースの構成変更を IM and Presence Service SIP プロキシに通知する、すべての構成エージェント アラーム。
CiscoUPInterclusterSyncAgent	クラスタ間ルーティングのために IM and Presence Service クラスタ間でエンドユーザ情報を同期化する、すべてのクラスタ間同期エージェント アラーム。
CiscoUPSPresenceEngine	可用性ステータスとユーザの通信機能に関する情報を収集する、すべてのプレゼンス エンジンアラーム。

名前	説明
CiscoUPSSIPProxy	ルーティング、要求者識別、およびトランスポートの相互接続に関するすべての SIP プロキシアラーム。
CiscoUPSSOAP	HTTPS を使用して外部クライアントとの間での安全な SOAP インターフェイスを提供する、すべての Simple Object Access Protocol (SOAP) アラーム。
CiscoUPSSyncAgent	Unified Communications Manager との IM and Presence Service データの同期を保つすべての Sync Agent アラーム。
CiscoUPXCP	IM and Presence Service 上の XCP コンポーネントとサービスのステータスに関する情報を収集するすべての XCP アラーム。
CiscoUPServerRecoveryManager	プレゼンス冗長グループ内のノード間のフェールオーバーおよびフォールバック プロセスに関するすべての Server Recovery Manager アラーム。
CiscoUPReplWatcher	IDS 複製状態をモニタするすべての ReplWatcher アラーム。
CiscoUPXCPCConfigManager	XCP コンポーネントに関係するすべての Cisco XCP Config Manager アラーム定義。

アラーム情報には、説明と推奨されるアクションが含まれているのに加えて、ローカル IM and Presence Service ノード以外の問題についてもトラブルシューティングを行うのに役立つ、アプリケーション名、サーバ名などが含まれています。

IM and Presence Service に固有のアラームの詳細については、『*System Error Messages for IM and Presence on Cisco Unified Communications Manager*』を参照してください。

CiscoSyslog ファイル内のデフォルトのアラーム

次の表に、アラーム設定なしで CiscoSyslog ファイルでトリガーされるデフォルトのアラームの説明を示します。

表 12: CiscoSyslog ファイル内のデフォルトのアラーム

名前	説明
CLM_IPSecCertUpdated	変更が発生したため、クラスタ内のピア ノードから IPSec 自己署名証明書がインポートされました。

名前	説明
CLM_IPAddressChange	クラスタ内のピアノードのIPアドレスが変更されました。
CLM_PeerState	クラスタ内の別のノードとのClusterMgrのセッション状態が、現在の状態に変更されました。
CLM_MsgIntChkError	ClusterMgr は、メッセージの整合性チェックに失敗したメッセージを受信しました。 これは、クラスタ内の別のノードが誤ったセキュリティパスワードで設定されていることを示す場合があります。
CLM_UnrecognizedHost	ClusterMgr は、このクラスタ内でノードとして設定されていない IP アドレスからメッセージを受信しました。
CLM_ConnectivityTest	Cluster Manager により、ネットワーク エラーが検出されました。
ServiceActivated	このサービスはアクティブになっています。
ServiceDeactivated	このサービスは現在非アクティブになっています。
ServiceActivationFailed	このサービスをアクティブにできませんでした。
ServiceDeactivationFailed	このサービスを非アクティブにできませんでした。
ServiceFailed	サービスが突然終了しました。サービスマネージャは再起動を試みます。
ServiceStartFailed	このサービスを開始できませんでした。サービスマネージャは、サービスを再度開始しようとします。
ServiceStopFailed	選定の再試行後に、指定されたサービスを停止できません。サービスは停止済みとしてマークされます。
ServiceRestartFailed	指定されたサービスを再起動できません。
ServiceExceededMaxRestarts	最大再起動の試行後でも、サービスを開始できませんでした。

名前	説明
FailedToReadConfig	設定ファイルの読み込みに失敗しました。設定ファイルが壊れている可能性があります。
MemAllocFailed	メモリの割り当てに失敗しました。
SystemResourceError	システム コールに失敗しました。
ServiceManagerUnexpectedShutdown	予期しない終了後にサービスマネージャが正常に再起動しました。
OutOfMemory	プロセスからオペレーティングシステムに対してメモリが要求されていますが、使用可能なメモリが不足しています。
作成-DST-ルール-ファイル-CLI	新しい DST ルールファイルが cli から生成されます。電話機を再起動する必要があります。電話機を再起動しないと、DST の開始/停止の日付が間違ってしまうます。
作成-DST-ルールファイル-ブートアップ	新しい DST ルールファイルがブートアップ中に生成されます。電話機を再起動する必要があります。電話機を再起動しないと、DST の開始日/終了日が間違った日付になります。
作成-DST-ルールファイル-CRON	新しい DST ルールファイルが cron から生成されます。電話機を再起動する必要があります。電話機を再起動しないと、DST の開始日/終了日が間違った日付になります。
PermissionDenied	このプロセスにはこの操作を実行する権限がないため、この操作を完了できませんでした。
ServiceNotInstalled	実行可能ファイルの開始が試行されていますが、サービス制御マネージャでサービスとして設定されていないため、開始できません。サービス名は %s です。
ServiceStopped	サービスが停止しました。
ServiceStarted	サービスが開始されました。
ServiceStartupFailed	サービスが開始されました。
FileWriteError	プライマリ ファイルパスに書き込めませんでした。



第 12 章

監査ログ

- [監査ログ \(137 ページ\)](#)

監査ログ

監査ログを使用すると、監査用の別のログ ファイルにシステムの設定変更が記録されます。

監査ロギング (標準)

監査ロギングが有効になっているが、詳細監査ロギングオプションが選択されていない場合、システムは標準の監査ロギング用に設定されます。

標準監査ロギングを使用すると、監査用の別のログファイルにシステムの設定変更が記録されます。Cisco Audit Event サービスは、サービス提供 GUI の [コントロールセンター-ネットワークサービス (Control Center-Network Services)] の下に表示され、ユーザによって行われた、またはユーザアクションの結果として、システムに対する設定変更をモニタしてログに記録します。

監査ログの設定を行うには、Serviceability GUI の [監査ログの設定 (Audit Log Configuration)] ウィンドウにアクセスします。

標準監査ロギングの構成は次のとおりです。

- 監査ロギングフレームワーク：このフレームワークは、監査ログに監査イベントを書き込むためにアラームライブラリを使用する API で構成されます。GenericAlarmCatalog.xml として定義されたアラームカタログがこれらのアラームに適用されます。システムコンポーネントごとに独自のロギングが提供されます。

以下に、アラームを送信するために Unified Communications Manager のコンポーネントを使用することが API の例を示します。

```
User ID: CCMAAdministratorClient IP Address: 172.19.240.207 Severity: 3
EventType: ServiceStatusUpdated ResourceAccessed: CCMSERVICE EventStatus:
Successful Description: CallManager Service status is stopped
```

- 監査イベントロギング：監査イベントとは、記録する必要があるあらゆるイベントを指します。次に、監査イベントの例を示します。

```
CCM_TOMCAT-GENERIC-3-AuditEventGenerated: Audit Event Generated
UserID:CCMAdministrator Client IP Address:172.19.240.207 Severity:3
EventType:ServiceStatusUpdated ResourceAccessed: CCMService
EventStatus:Successful Description: Call Manager Service status is stopped
App ID:Cisco Tomcat Cluster ID:StandAloneCluster Node ID:sa-cml-3
```



ヒント 監査イベントのロギングは、デフォルトでは一元的に管理され、有効化されることに注意してください。Syslog Audit というアラームモニタによってログが書き込まれます。デフォルトでは、ログはローテーションするように設定されています。AuditLogAlarmMonitor が監査イベントを書き込むことができない場合、AuditLogAlarmMonitor はこのエラーを重大なエラーとして syslog ファイルに記録します。Alert Manager は、このエラーを、「シビラティ (重大度) が一致した」アラートの一部として報告します。イベントロギングが失敗した場合も実際の動作は継続されます。監査ログはすべて、Cisco Unified Real-Time Monitoring Tool の Trace and Log Central から収集、表示、および削除されます。

シスコユニファイドサービス標準イベントロギング

Cisco Unified Serviceability では次のイベントがログに記録されます。

- サービスのアクティブ化、非アクティブ化、起動、または停止。
- トレース設定およびアラーム設定の変更。
- SNMP 設定の変更。
- CDR 管理の変更 (Cisco Unified Communications Manager のみ)。
- サービスアビリティ レポートのアーカイブのレポートの参照。このログは、レポート用ノードで表示されます。(Unified Communications Manager のみ)

Cisco Unified Real-Time Monitoring Tool の標準イベント ロギング

Cisco Unified Real-Time Monitoring Tool では、監査イベント アラームを含む次のイベントがログに記録されます。

- アラートの設定
- アラートの中断
- 電子メールの設定
- ノードアラート ステータスの設定
- アラートの追加
- アラートの追加アクション

- アラートのクリア
- アラートのイネーブル化
- アラートの削除アクション
- アラートの削除

Unified Communications Manager 標準イベント ロギング

Cisco CDR Analysis and Reporting (CAR) では、以下のイベントに関する監査ログが作成されます。

- ローダのスケジューリング
- 日次、週次、月次レポートのスケジューリング
- メールパラメータの設定
- ダイアルプラン設定
- ゲートウェイの設定
- システムプリファレンスの設定
- 自動消去の設定
- 接続時間、時刻、および音声品質の評価エンジンの設定
- QoS の設定
- 事前生成レポートの自動生成/アラートの設定
- 通知限度の設定

Cisco Unified CM Administration の標準イベントロギング

次のイベントは、Cisco Unified Communications Manager Administration のさまざまなコンポーネントに対して記録されます。

- ユーザのログイン/ログアウト
- ユーザのロールメンバーシップの更新（ユーザの追加、ユーザの削除、またはユーザのロールの更新）
- ロールの更新（新しいロールの追加、削除、または更新）
- デバイスの更新（電話機およびゲートウェイ）
- サーバ設定の更新（アラームまたはトレースの設定、サービスパラメータ、エンタープライズパラメータ、IP アドレス、ホスト名、イーサネット設定の変更、および Unified Communications Manager サーバの追加または削除）。

Cisco Unified Communications セルフ ケア ポータルの標準イベント ロギング

Cisco Unified Communications セルフ ケア ポータルに対するユーザ ロギング (ユーザ ログインとユーザ ログアウト) イベントが記録されます。

コマンドラインインターフェイスの標準イベントロギング

コマンドラインインターフェイスで実行されたすべてのコマンドがログに記録されます (Unified Communications Manager と Cisco Unity Connection の両方)。

Cisco Unity Connection Administration の標準イベント ロギング

Cisco Unity Connection Administration では次のイベントがログに記録されます。

- ユーザのログイン/ログアウト
- すべての設定変更 (ユーザ、連絡先、コール管理オブジェクト、ネットワーク、システム設定、テレフォニーなど)
- タスク管理 (タスクの有効化/無効化)
- 一括管理ツール (一括作成、一括削除)
- カスタム キーパッド マップ (マップの更新)

Cisco Personal Communications Assistant (Cisco PCA) の標準イベント ロギング

Cisco Personal Communications Assistant クライアントでは次のイベントがログに記録されます。

- ユーザのログイン/ログアウト
- Messaging Assistant で行われたすべての設定変更

Cisco Unity Connection Serviceability の標準イベント ロギング

Cisco Unity Connection Serviceability では次のイベントがログに記録されます。

- ユーザのログイン/ログアウト。
- すべての設定変更。
- サービスのアクティブ化、非アクティブ化、開始、または停止。

Representational State Transfer API を使用する Cisco Unity Connection クライアントのイベント ロギング

Representational State Transfer (REST) API を使用する Cisco Unity Connection クライアントでは次のイベントがログに記録されます。

- ユーザのログイン (ユーザの API 認証)。
- Cisco Unity Connection プロビジョニング インターフェイスを使用する API 呼び出し。

Cisco Unified IM and Presence Serviceability の標準イベント ロギング

Cisco Unified IM and Presence Serviceability では次のイベントがログに記録されます。

- サービスのアクティブ化、非アクティブ化、起動、または停止
- トレース設定およびアラーム設定の変更
- SNMP 設定の変更
- サービスアビリティ レポートのアーカイブ内のレポートの参照 (このログは、レポート用ノードで表示されます)

Cisco Unified IM and Presence リアルタイムモニタリングツール標準イベントロギング

Cisco Unified IM and Presence Real-Time Monitoring Tool では、監査イベント アラームを含む次のイベントがログに記録されます。

- アラートの設定
- アラートの中断
- 電子メールの設定
- ノード アラート ステータスの設定
- アラートの追加
- アラートの追加アクション
- アラートのクリア
- アラートのイネーブル化
- アラートの削除アクション
- アラートの削除

Cisco IM and Presence Administration の標準イベント ロギング

以下のイベントは、Cisco Unified Communications Manager 管理のさまざまなコンポーネントに対して記録されます。

- 管理者のロギング (Administration、OS Administration、Disaster Recovery System、Reporting などの IM and Presence のインターフェイスへのログインおよびログアウト)
- ユーザのロール メンバーシップの更新 (ユーザの追加、ユーザの削除、またはユーザのロールの更新)
- ロールの更新 (新しいロールの追加、削除、または更新)
- デバイスの更新 (電話機およびゲートウェイ)

- サーバ設定の更新（アラームまたはトレースの設定、サービスパラメータ、エンタープライズパラメータ、IPアドレス、ホスト名、イーサネット設定の変更、およびIM and Presenceサーバの追加または削除）

IM and Presence アプリケーションの標準イベントロギング

IM and Presence アプリケーションのさまざまなコンポーネントでは、次のイベントがログに記録されます。

- IM クライアントへのエンドユーザのログイン（ユーザのログイン/ログアウト、およびログイン試行の失敗）
- IM チャット ルームへのユーザの入室および退室
- IM チャットルームの作成と破壊

コマンドラインインターフェイスの標準イベントロギング

コマンドライン インターフェイスで実行されたすべてのコマンドがログに記録されます。

監査ロギング（詳細）

詳細な監査ロギングは、標準(デフォルト)の監査ログに保存されていない追加の設定変更をログに記録するオプション機能です。標準監査ログに保存されるすべての情報に加えて、詳細監査ロギングには、変更された値も含め、追加、更新、または削除された設定項目も保存されます。詳細監査ロギングはデフォルトで無効になっていますが、[監査ログ設定 (Audit Log Configuration)] ウィンドウで有効にすることができます。

監査ログのタイプ

システム監査ログ

システム監査ログでは、Linux OS ユーザの作成、変更、削除、ログの改ざん、およびファイルまたはディレクトリの権限に対するあらゆる変更をトレースします。このタイプの監査ログは、収集されるデータが大量になるためにデフォルトでディセーブルになっています。この機能を有効にするには、CLI を使用して、手動でユーティリティの `auditd` を有効にする必要があります。システム監査ログ機能をイネーブルにすると、Real-Time Monitoring Tool の [Trace & Log Central] を使用して、選択したログの収集、表示、ダウンロード、削除を実行できます。システム監査ログは、`vos-audit`の形式で実行されます。

この機能をイネーブルにする方法については、『Cisco Unified Communications Solutions コマンドライン インターフェイス リファレンス ガイド』を参照してください。Real-Time Monitoring Tool から収集したログを操作する方法については、『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。

アプリケーション監査ログ

アプリケーション監査ログは、ユーザが行った、またはユーザアクションの結果として行われたシステムへの設定変更をモニタし、記録します。



- (注) アプリケーションの監査ログ (Linux auditd) は、CLIからのみイネーブルまたはディセーブルにすることができます。このタイプの監査ログの設定は、Real-Time Monitoring Tool による vos-audit.log の収集以外は変更できません。

データベース監査ログ

データベース監査ログは、ログインなど、Informix データベースへのアクセスに関連するすべてのアクティビティを追跡します。

監査ログ設定タスク フロー

監査ロギングを設定するには、次のタスクを実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	監査ロギングのセットアップ (144 ページ)	[監査ログの設定 (Audit Log Configuration)] ウィンドウで監査ログの設定を行います。リモート監査ロギングを使用するかどうか、および詳細な監査ロギングオプションを使用するかどうかを設定できます。
ステップ 2	リモート監査ログの転送プロトコルの設定 (145 ページ)	オプション。リモート監査ロギングを設定した場合は、転送プロトコルを設定します。通常の動作モードのシステム デフォルトは UDP ですが、TCP または TLS を設定することもできます。
ステップ 3	アラート通知用の電子メール サーバの設定 (145 ページ)	オプション。RTMT で、電子メールアラート用の電子メール サーバをセットアップします。
ステップ 4	電子メールアラートの有効化 (146 ページ)	オプション。次の電子メールアラートのいずれかを設定します。 <ul style="list-style-type: none"> リモート監査ロギングが TCP で設定されている場合は、TCPRemoteSyslogDeliveryFailed ア

	コマンドまたはアクション	目的
		<p>ラート用の電子メール通知をセットアップします。</p> <ul style="list-style-type: none"> • TLSでリモート監査ロギングが設定されている場合は、TLSRemoteSyslogDeliveryFailedアラートの電子メール通知を設定します。
ステップ 5	プラットフォーム ログのリモート監査ロギングの設定 (147 ページ)	プラットフォーム監査ログおよびリモートサーバログのリモート監査ロギングを設定します。これらのタイプの監査ログでは、FileBeat クライアントと外部 logstash サーバを設定する必要があります。

監査ロギングのセットアップ

始める前に

リモート監査ロギングでは、事前に、リモート syslog サーバをセットアップし、間にあるゲートウェイへの接続も含め、各クラスタノードとリモート syslog サーバ間で IPsec を設定しておく必要があります。IPsec 設定については、『Cisco IOS Security Configuration Guide』を参照してください。

手順

-
- ステップ 1 Cisco Unified Serviceability で、[ツール (Tools)] > [監査ログ設定 (Audit Log Configuration)] を選択します。
 - ステップ 2 [サーバ (Server)] ドロップダウンメニューから、クラスタ内のサーバを選択し、[実行 (Go)] をクリックします。
 - ステップ 3 すべてのクラスタノードを記録するには、[すべてのノードに適用 (Apply to All Nodes)] チェックボックスをオンにします。
 - ステップ 4 [サーバ名 (Server Name)] フィールドに、リモート syslog サーバの IP アドレスまたは完全修飾ドメイン名を入力します。
 - ステップ 5 これはオプションです。変更された項目と変更された値も含め、設定更新を記録するには、[詳細監査ロギング (Detailed Audit Logging)] チェックボックスをオンにします。
 - ステップ 6 [監査ログ設定 (Audit Log Configuration)] ウィンドウの残りのフィールドに値を入力します。フィールドとその説明を含むヘルプについては、オンラインヘルプを参照してください。
 - ステップ 7 [保存 (Save)] をクリックします。
-

次のタスク

[リモート監査ログの転送プロトコルの設定 \(145 ページ\)](#)

リモート監査ログの転送プロトコルの設定

リモート監査ログ用の転送プロトコルを変更するには、次の手順を使用します。システム デフォルトは UDP ですが、に設定し直すこともできます。TCP または TLS。

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 `utils remotesyslog show protocol` コマンドを実行して、どのプロトコルが設定されているかを確認します。

ステップ 3 このノード上でプロトコルを変更する必要がある場合は、次の手順を実行します。

- TCP を設定するには、`utils remotesyslog set protocol tcp` コマンドを実行します。
- UDP を設定するには、`utils remotesyslog set protocol udp` コマンドを実行します。
- TLS を設定するには、`utils remotesyslog set protocol tls` コマンドを実行します。

TLS 接続を設定するには、セキュリティ証明書を syslog サーバから Unified Communications Manager および IM and Presence サービス上の Tomcat 信頼ストアにアップロードする必要があります。

(注) コモンクライテリア モードでは、厳密なホスト名検証が使用されます。そのため、証明書と一致する完全修飾ドメイン名 (FQDN) でサーバを設定する必要があります。

ステップ 4 プロトコルを変更した場合は、ノードを再起動します。

ステップ 5 すべての Unified Communications Manager および IM and Presence サービスのクラスタ ノードでこの手順を繰り返します。

次のタスク

[アラート通知用の電子メール サーバの設定 \(145 ページ\)](#)

アラート通知用の電子メール サーバの設定

アラート通知用の電子メール サーバをセットアップするには、次の手順を使用します。

手順

ステップ 1 Real-Time Monitoring Tool のシステム ウィンドウで、[アラート セントラル (Alert Central)] をクリックします。

- ステップ2 [システム (System)] > [ツール (Tools)] > [アラート (Alert)] > [電子メール サーバの設定 (Config Email Server)] の順に選択します。
- ステップ3 [メールサーバ設定 (Mail Server Configuration)] ポップアップで、メールサーバの詳細を入力します。
- ステップ4 [OK] をクリックします。
-

次のタスク

[電子メールアラートの有効化 \(146 ページ\)](#)

電子メールアラートの有効化

リモート監査ロギングを TCP または TLS で設定した場合は、次の手順を使用して、送信障害を通知する電子メールアラートを設定します。

手順

- ステップ1 Real-Time Monitoring Tool の [システム (System)] 領域で、[アラートセントラル (Alert Central)] をクリックします。
- ステップ2 **Alert Central** ウィンドウで、
- TCP でリモート監査ロギングを使用する場合は、**TCPRemoteSyslogDeliveryFailed** を選択します。
 - TLS でリモート監査ロギングを使用する場合は、**TLSRemoteSyslogDeliveryFailed** を選択します。
- ステップ3 [システム (System)] > [ツール (Tools)] > [アラート (Alert)] > [アラートアクションの設定 (Config Alert Action)] の順に選択します。
- ステップ4 [アラートアクション (Alert Action)] ポップアップで、[デフォルト (Default)] を選択して、[編集 (Edit)] をクリックします。
- ステップ5 [アラートアクション (Alert Action)] ポップアップで、受信者を追加します。
- ステップ6 ポップアップウィンドウで、電子メールアラートを送信するアドレスを入力して、[OK] をクリックします。
- ステップ7 [アラートアクション (Alert Action)] ポップアップで、アドレスが [受信者 (Recipients)] に表示されていることと、[有効 (Enable)] チェックボックスがオンになっていることを確認します。
- ステップ8 [OK] をクリックします。
-

プラットフォーム ログのリモート監査ロギングの設定

プラットフォーム監査ログ、リモートサポートログ、および一括管理 csv ファイルのリモート監査ロギングサポートを追加するには、次のタスクを実行します。これらのタイプのログでは、FileBeat クライアントと logstash サーバが使用されます。

始める前に

外部 logstash サーバがセットアップされていることを確認します。

手順

	コマンドまたはアクション	目的
ステップ 1	Logstash サーバ情報の設定 (147 ページ)	IP アドレス、ポート、ファイルタイプなどの外部 logstash サーバ詳細で FileBeat クライアントを設定します。
ステップ 2	FileBeat クライアントの設定 (147 ページ)	リモート監査ロギング用の FileBeat クライアントを有効にします。

Logstash サーバ情報の設定

次の手順を使用して、IP アドレス、ポート番号、ダウンロード可能なファイル タイプなどの外部 Logstash サーバ情報で FileBeat クライアントを設定します。

始める前に

外部 Logstash サーバがセットアップされていることを確認します。

手順

-
- ステップ 1 コマンドライン インターフェイスにログインします。
 - ステップ 2 `utils FileBeat configure` コマンドを実行します。
 - ステップ 3 画面上の指示に従って、Logstash サーバの詳細を設定します。
-

FileBeat クライアントの設定

プラットフォーム監査ログ、リモートサポートログ および一括管理 CSV ファイルのアップロード用の FileBeat クライアントを有効または無効にするには、次の手順を使用します。

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 **utils FileBeat status** コマンドを実行し、Filebeat クライアントが有効になっているかどうかを確認します。

ステップ 3 次のコマンドの 1 つを実行します。

- クライアントを有効にするには、**utils FileBeat enable** コマンドを実行します。
- クライアントを無効にするには、**utils FileBeat disable** コマンドを実行します。

(注) TCP はデフォルトの転送プロトコルです。

ステップ 4 これはオプションです。転送プロトコルとして TLS を使用するには、次の手順を実行します。

- 転送プロトコルとして TLS を有効にするには、**utils FileBeat tls enable** コマンドを実行します。
- 転送プロトコルとして TLS を無効にするには、**utils FileBeat tls disable** コマンドを実行します。

(注) TLS を使用するには、セキュリティ証明書を logstash サーバから Unified Communications Manager および IM and Presence サービス上の tomcat 信頼ストアにアップロードする必要があります。

ステップ 5 各ノードでこの手順を繰り返します。

これらのコマンドをすべてのノードで同時に実行しないでください。

監査ログの構成時の設定

はじめる前に

監査ロールを割り当てられたユーザだけが監査ログの設定を変更できることに注意してください。デフォルトでは、Unified Communications Manager の新規インストールおよびアップグレード後、CCMAdministrator が監査ロールを所有します。CCMAdministrator は、Cisco Unified Communications Manager Administration の [User Group Configuration] ウィンドウで標準監査ユーザグループに監査権限を持つユーザを割り当てることができます。その後必要であれば、標準監査ユーザグループから CCMAdministrator を削除できます。

IM and Presence サービスの場合、管理者は、新規インストールとアップグレード後に監査ロールを所有し、監査権限を持つユーザを標準監査ユーザグループに割り当てることができます。

Cisco Unity Connection の場合、インストール時に作成されたアプリケーション管理アカウントが Audit Administrator ロールに割り当てられます。このアカウントは、他の管理者ユーザをこのロールに割り当てることができます。このアカウントから Audit Administrator ロールを削除することもできます。

Standard Audit Log Configuration ロールには、監査ログを削除する権限と、Cisco Unified Real-Time Monitoring Tool、IM and Presence Real-Time Monitoring Tool、Trace Collection Tool、Real-Time Monitoring Tool (RTMT) アラート設定、Serviceability ユーザインターフェイスのコントロールセンター - ネットワーク サービス、RTMT プロファイルの保存、Serviceability ユーザイン

ターフェイスの監査設定、監査トレースというリソースへの読み取り/更新権限が与えられません。

Standard Audit Log Configuration ロールには、監査ログを削除する権限と、Cisco Unified RTMT、Trace Collection Tool、RTMT アラート設定、Cisco Unified Serviceability のコントロールセンター-ネットワーク サービス、RTMT プロファイルの保存、Cisco Unified Serviceability の監査設定、監査トレースというリソースへの読み取り/更新権限が与えられます。

Cisco Unity Connection の Audit Administrator ロールに割り当てられたユーザは、Cisco Unified RTMT で監査ログを表示、ダウンロード、および削除できます。

Cisco Unified Communications Manager のロール、ユーザ、およびユーザグループの詳細については、*Cisco Unified Communications Manager 管理ガイド*を参照してください。

Cisco Unity Connection のロールとユーザの詳細については、『*User Moves, Adds, and Changes Guide for Cisco Unity Connection*』を参照してください。

IM and Presenceのロール、ユーザ、ユーザグループの詳細は、*Unified Communications Manager の Configuration and Administration of IM and Presence Service* の設定および管理を参照してください。

次の表に、Cisco Unified Serviceability の [監査ログの設定 (Audit Log Configuration)] ウィンドウで設定できる設定について説明します。

表 13: 監査ログの構成時の設定

フィールド	説明
サーバの選択	
サーバ (Server)	監査ログを設定するサーバ (ノード) を選択し、[移動 (Go)]をクリックします。
すべてのノードに適用 (Apply to All Nodes)	クラスタのすべてのノードに監査ログ設定を適用する場合は、[すべてのノードに適用 (Apply to All Nodes)] チェックボックスをオンにします。
アプリケーション監査ログの設定	

フィールド	説明
監査ログを有効にする (Enable Audit Log)	<p>このチェックボックスをオンにすると、監査ログがアプリケーション監査ログに対して作成されます。</p> <p>Unified Communications Managerの場合、アプリケーション監査ログは、Cisco Unified Communications Manager 管理、Cisco Unified RTMT、Cisco Unified Communications Manager CDR Analysis and Reporting および Cisco Unified Serviceabilityなどの Unified Communications Manager ユーザ インターフェイスの設定の更新をサポートします。</p> <p>IM and Presence Service の場合、アプリケーション監査ログは Unified Communications Manager IM and Presence 管理、Cisco Unified IM and Presence Real-Time Monitoring Tool、Cisco Unified IM and Presence Serviceability などの IM and Presence ユーザ インターフェイスの設定更新をサポートします。</p> <p>Cisco Unity Connection の場合、アプリケーション監査ログは Cisco Unity Connection Administration、Cisco Unity Connection Serviceability、Cisco Personal Communications Assistant、接続 REST API を使用するクライアントなどの Cisco Unity Connection ユーザ インターフェイスの設定更新をサポートします。</p> <p>この設定は、デフォルトで有効と表示されます。</p> <p>(注) ネットワークサービス監査イベントサービスが実行されている必要があります。</p>
消去を有効にする (Enable Purging)	<p>Log Partition Monitor (LPM) は、[消去を有効にする (Enable Purging)] オプションを確認して監査ログを消去する必要があるかどうかを判断します。このチェックボックスをオンにすると、共通パーティションのディスク使用率が上限を超えるたびに LPM によって RTMT のすべての監査ログファイルが消去されます。ただし、このチェックボックスをオフにして消去を無効にすることができます。</p> <p>消去が無効の場合、監査ログの数は、ディスクがいっぱいになるまで増加し続けます。このアクションは、システムの中断を引き起こす可能性があります。[消去を有効にする (Enable Purging)] チェックボックスをオフにすると、消去の無効化のリスクを説明するメッセージが表示されます。このオプションは、アクティブパーティションの監査ログに使用可能なことに注意してください。監査ログが非アクティブパーティションにある場合、ディスク使用率が上限を上回ると消去されます。</p> <p>監査ログにアクセスするには、RTMT の [Trace & Log Central][監査ログ (Audit Logs)]> を選択します。</p> <p>(注) ネットワーク サービス Cisco Log Partition Monitoring Tool が動作している必要があります。</p>

フィールド	説明
ログローテーションを有効にする (Enable Log Rotation)	<p>システムは、このオプションを読み取り、監査ログファイルをローテーションする必要があるか、または新しいファイルの作成を続行するかを判断します。ファイルの最大数は 5000 を超えることはできません。[ログローテーションを有効にする (Enable Log Rotation)] チェックボックスをオンにすると、監査ログファイルの最大数に達すると最も古いファイルが上書きされます。</p> <p>ヒント ログローテーションを無効 (オフ) にすると、監査ログは [最大ファイル数 (Maximum No. of Files)] 設定を無視します。</p>
詳細監査ロギング (Detailed Audit Logging)	このチェックボックスをオンにすると、システムは詳細監査ログに対して有効にされます。詳細な監査ログは、通常の監査ログと同じ項目を提供しますが、設定の変更も含まれます。たとえば、監査ログには、変更された値を含む、追加、更新、および削除された項目が含まれます。
サーバ名	<p>Syslog メッセージ受信のために使用する、リモート Syslog サーバの名前または IP アドレスを入力します。サーバ名が指定されていない場合、Cisco Unified IM and Presence Serviceability は Syslog メッセージを送信しません。ノードは他のサーバからの Syslog メッセージを受け付けないため、Unified Communications Manager ノードを通知先として指定しないでください。</p> <p>これは、IM and Presence Service にのみ適用されます。</p>
リモート Syslog 監査イベントレベル (Remote Syslog Audit Event Level)	<p>リモート Syslog サーバの、対象となる Syslog メッセージのシビラティ (重大度) を選択します。選択したシビラティ (重大度) 以上のすべての Syslog メッセージが、リモート Syslog に送信されます。</p> <p>これは、IM and Presence Service にのみ適用されます。</p>
最大ファイル数 (Maximum No. of Files)	ログに含めるファイルの最大数を入力します。デフォルト設定は 250 です。最大数は 5000 です。
最大ファイルサイズ (Maximum File Size)	監査ログの最大ファイルサイズを入力します。ファイルサイズの値は 1 MB～10 MB の範囲内にする必要があります。1～10 の間の数を指定します。

フィールド	説明
ログローテーションの上書きに近づいた場合の警告しきい値 (%)	<p>監査ログが上書きされるレベルに達すると、警告が送信されます。システムがアラートを送信するしきい値を設定するには、このフィールドを使用します。</p> <p>たとえば、250ファイルのデフォルト設定を2MBに、警告しきい値として80%を使用すると、システムは200ファイル(80%)でアラームを送信します。監査ログの合計が累積されました。監査履歴を保持する場合は、RTMTを使用してログを取得してから、システムがそれらを上書きする必要があります。RTMTには、収集後にファイルを削除するオプションが用意されています。</p> <p>1～99%の範囲で値を入力します。デフォルトは80%です。このフィールドを設定する場合は、[ログローテーションの有効化 (Enable Log Rotation)] オプションもオンにする必要があります。</p> <p>(注) 監査ログに割り当てられる合計ディスク領域は、最大数です。ファイルの最大サイズを乗算します。ディスク上の監査ログのサイズが、割り当てられた合計ディスク領域のこの割合を超えた場合、システムはAlert Centralでアラームを発生させます。</p>
データベース監査ログ フィルタ設定	
監査ログを有効にする (Enable Audit Log)	<p>このチェックボックスをオンにすると、監査ログが Unified Communications Manager および Cisco Unity Connection データベースに作成されます。[デバッグ監査レベル (Debug Audit Level)] の設定とともにこの設定を使用します。これにより、データベースの特定の側面に対してログを作成できます。</p>

フィールド	説明
デバッグ監査レベル (Debug Audit Level)	<p>この設定では、ログで監査するデータベースの側面を選択できます。ドロップダウン リスト ボックスから、次のオプションのいずれかを選択します。各監査ログ フィルタ レベルは累積的であることに注意してください。</p> <ul style="list-style-type: none"> • [スキーマ (Schema)] : 監査ログ データベースの設定の変更 (たとえば、データベース テーブルのカラムや行) を追跡します。 • 管理タスク : Unified Communications Manager システムに対するすべての管理上の変更 (たとえば、システム保全のためのあらゆる変更など) およびすべてのスキーマを追跡します。 <p>ヒント ほとんどの管理者は [管理タスク (Administrative Tasks)] 設定を無効にしたままにします。監査が必要なユーザに対しては、[データベースの更新 (Database Updates)] レベルを使用します。</p> <ul style="list-style-type: none"> • [データベースの更新 (Database Updates)] : データベースのすべての変更、および [スキーマ (Schema)] のすべての変更と [管理タスク (Administrative Tasks)] のすべての変更を追跡します。 • データベースの読み取り : システムへのすべての読み取りと、すべてのスキーマ変更、管理タスク変更、データベース更新のすべての変更を追跡します。 <p>ヒント Unified Communications Manager または Cisco Unity Connection システムを簡単に確認する場合にのみ、データベースの読み取りレベルを選択します。このレベルでは、大量のシステム リソースを消費するため、短時間だけ使用してください。</p>
監査ログローテーションを有効にする (Enable Audit Log Rotation)	<p>システムはこのオプションを読み取り、データベースの監査ログ ファイルをローテーションする必要があるか、または新しいファイルの作成を続行するかどうかを判断します。[監査ログローテーションを有効にする (Enable Audit Log Rotation)] オプションのチェックボックスをオンにすると、監査ログファイルが最大数に達すると最も古いファイルが上書きされます。</p> <p>この設定のチェックボックスがオフの場合、監査ログでは [最大ファイル数 (Maximum No. of Files)] 設定は無視されます。</p>
最大ファイル数 (Maximum No. of Files)	<p>ログに含めるファイルの最大数を入力します。[最大ファイル数 (Maximum No. of Files)] 設定に入力した値が、[ログローテーション時に削除されるファイル数 (No. of Files Deleted on Log Rotation)] 設定に入力した値を上回っていることを確認します。</p> <p>4 (最小) ~ 40 (最大) の値を入力できます。</p>

フィールド	説明
ログローテーション時に削除されるファイル数 (No. of Files Deleted on Log Rotation)	<p>データベース監査ログのローテーションが発生したときにシステムが削除できるファイルの最大数を入力します。</p> <p>このフィールドに入力できる最小値は1です。最大値は [最大ファイル数 (Max No. of Files)] 設定に入力した値よりも2低い数値です。たとえば、[最大ファイル数 (Max No. of Files)] フィールドに40を入力した場合、[ログローテーション時に削除されるファイル数 (No. of Files Deleted on Log Rotation)] フィールドに入力できる最大数は38です。</p>
デフォルトに設定 (Set to Default)	<p>[デフォルトに設定 (Set to Default)] ボタンは、デフォルト値を指定します。詳細なトラブルシューティングのために別のレベルに設定する必要がある場合を除き、監査ログをデフォルトモードに設定することを推奨します。[デフォルトに設定 (Set To Default)] オプションは、ログファイルによって使用されるディスク領域を最小化します。</p>



注意 有効にすると、データベースロギングは短時間で大量のデータを生成することがあります。特に、デバッグ監査レベルが**データベースの更新**または**データベースの読み取り**に設定されている場合です。これにより、使用量が多いときにパフォーマンスが大幅に低下する可能性があります。一般に、データベースロギングを無効のままにしておくことをお勧めします。データベースの変更を追跡するためにロギングを有効にする必要がある場合は、**データベースの更新**レベルを使用して短時間だけ実行することをお勧めします。同様に、管理ロギングはWebユーザインターフェイスの全体的なパフォーマンスに影響します。特に、データベースエントリをポーリングする場合(たとえば、データベースから250デバイスをプルする場合)に影響します。



第 13 章

Call Home

- [Call Home](#) (155 ページ)

Call Home

この章では、Unified Communications Manager Call Home サービスの概要と Unified Communications Manager Call Home 機能を設定する方法について説明します。Call Home 機能を使用すると、Smart Call Home バックエンドサーバと通信し、診断アラート、インベントリなどのメッセージを送信できます。

Smart Call Home

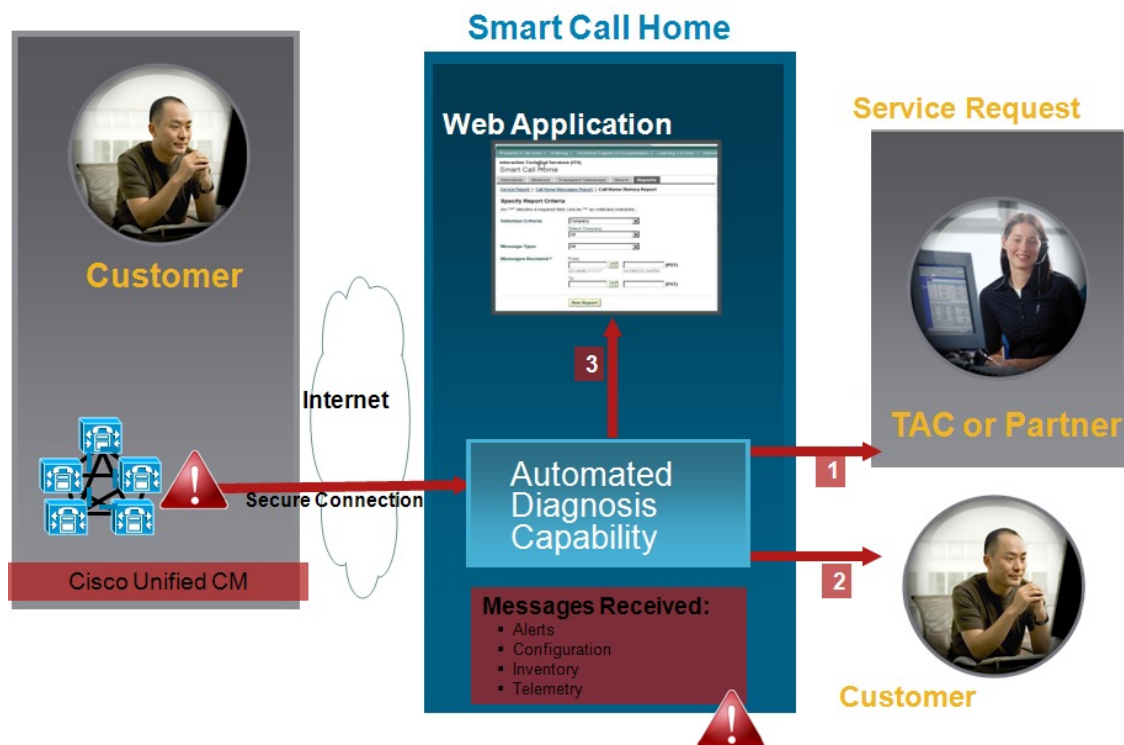
Smart Call Home では、さまざまなシスコ デバイスを対象として予防的診断、リアルタイムアラート、および修復を実行し、ネットワークの可用性と運用効率を向上させます。Smart Call Home が有効化された Unified Communications Manager から診断アラート、インベントリ、その他のメッセージを受け取り、分析することでも、同様の結果が得られます。Unified Communications Manager のこの機能は、Unified Communications Manager Call Home と呼ばれます。

Smart Call Home の機能は次のとおりです。

- 次の機能によって予防的で迅速な問題解決を行い、ネットワークの可用性を向上させます。
 - 継続的なモニタリング、リアルタイムの予防的なアラート、および詳細な診断により、問題を迅速に特定する。
 - ネットワーク内のデバイスのタイプに特有のアラートを発生させ、潜在的な問題を認識できるようにします。Cisco Technical Assistance Center (TAC) のエキスパートに直接かつ自動的にアクセスして、重大な問題を迅速に解決します。
- ユーザに次の機能を提供して、運用効率を向上させます。
 - トラブルシューティングに要する時間を短縮し、人材を有効に活用する。

- 必要な情報に迅速に Web ベースでアクセスでき、ユーザが次のことを実行できるようにします。
 - Call Home のすべてのメッセージ、診断、推奨事項を 1 ヶ所で確認する。
 - サービス リクエスト ステータスを迅速に確認できます。
 - 全 Call Home デバイスの最新のインベントリおよび設定情報を表示する。

図 2: Cisco Smart Call Home の概要



239157

Smart Call Home には、次のタスクを実行するモジュールが含まれています。

- ユーザへの Call Home メッセージの通知。
- 影響分析と修正手順の提供。

Smart Call Home の詳細については、次の URL の Smart Call Home のページを参照してください。

http://www.cisco.com/en/US/products/ps7334/serv_home.html

Smart Call Home 証明書の更新に関する情報

Cisco リリース 10.5(2) 以降では、Smart Call Home 機能のサポートを継続するには、更新要求の都度、管理者が新しい証明書を手動でアップロードする必要があります。証明書のアップロードは、Cisco Unified Operating System (OS) 管理 Web GUI を使用して行うことができます。[セ

セキュリティ] > [証明書管理] > [証明書または証明書チェーンのアップロード]を開きます。証明書として **tomcat-trust** を選択して、保存した接続先から証明書をアップロードします。

以下の「.PEM」拡張子の証明書を tomcat-trust にアップロードする必要があります。



- (注) 管理者は、文字列全体をコピーして、「-----BEGIN CERTIFICATE----- and -----END CERTIFICATE-----」を含めてテキストファイルにペーストして、「.PEM」の拡張子で保存します。

-----BEGIN CERTIFICATE-----

MIIIFtZCCA5+gAwIBAgICBQkwDQYJKoZIhvcNAQEFBQAwrTELMaKGA1UEBhMCQk0x
GTAXBgNVBAoTEFF1b1ZhZGlzIEExpbWl0ZWQxGzAZBgNVBAMTElF1b1ZhZGlzIFJv
b3QgQ0EgMjAeFw0wNjExMjQxODI3MDBaFw0zMTExMjQxODIzMzNaMEUxCzAJBgNV
BAYTAKJNMRkwFwYDVQQKEExBRdW9WYWRpcyBMAW1pdGVkMRswGQYDVQQDEExJRdW9
WYWRpcyBSb290IENBIDIwggliMA0GCsqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQCa
GMpLlA0ALa8DKYrWd4HlRkwZr0In6spRlXzL4GtMh6QRr+jhiYaHv5+HBg6XJxg
Fyo6dIMzMh1hVBHL7avg5tKifvVrbxi3Cgst/ek+7wrGsxDp3MJGF/hd/aTa/55J
WpzmM+Yklvc/ulsrHHo1wtZn/qtmUIttKGAr79dgw8eTvI02kfN/+NsRE8Scd3bB
rrcCaoF6qUWD4gXmuVbBlDePSHFjluwXZQeVikvfj8ZaCuWw419eaxGrDPMf60Tp
+ARz8un+XJiM9XOva7R+zdRcAitMoEGylZUtQofX1bOQQ7dsE/He3fbE+Ik/0XX1
ksOR1YqI0JDs3G3eicJlcZaLDQP9nL9bFqyS2+r+eXyt66/3FsvbzSUR5R/7mp/i
Ucw6UwxI5g69yBR2BILmEROfcmMDBOAEenigGQLodKcftslWZvB1JdxnwQ5hYIiz
PtGo / KPaHbDRsSNU30R2be1B2MGyIrZTHN81Hdyhdyox5C315eXbyOD / 5YDXC2Og
/ zOhD7osFRXql7PSorW + 8oyWHhqPHWykYTe5hnMz15eWniN9ggqRMgeKh0bnpX5UH
oycR7hYQe7xFSkyyBNKr79X9DFHOUGoIMfmR2gyPZFwDwzqLID9ujWc9Otb + fVuI
yV77zGHcizN300QyNqliBIIWENieJ0f7OyHj + OsdWwIDAQABo4GwMIGtMA8GA1Ud
EwEB / wQFMAMBAf8wCwYDVR0PBAQDAgEGMB0GA1UdDgQWBQBqahGK8SEwzJQTU7tD2
A8QZRtGUazBuBgNVHSMEZzBlgBQahGK8SEwzJQTU7tD2A8QZRtGUa6FJpEwRTEL
MAKGA1UEBhMCQk0xGTAXBgNVBAoTEFF1b1ZhZGlzIEExpbWl0ZWQxGzAZBgNVBAMT
ElF1b1ZhZGlzIFJvY3QgQ0EgMoICBQkwDQYJKoZIhvcNAQEFBQAADggIBAD4Kfk2f
BlueornFdLwUvZ + YTRYPENvzbwCYMDbVHZF34tHLJRqUDGcdViXh9duqWNIAXINzn
g / iN / Ae42l9NLmeyhP3ZRPx3UIHmflTJDQyU / h2BwdBR5YM ++ CCJpNVjP4iH2Bl
fF / nJrP3MpCYUNQ3cVX2kiF495V5 + vgtJodmVjB3pjd4M1IQWK4 / YY7yarHvGH5K
WWPKjaJW1acvvFYfzbnB4vsKqBUfU16Y8Zsl0Q80m / DShcK + JDSV6IZUaUtl0Ha
B0 + pUNqQjZRG4T7wlp0QADj1O + hA4bRuVhogzG9Yje0uRY / W6ZM / 57Es3zrWIozc
hLsib9D45MY56QSIPMO661V6bYcZJPVSAfv4l7CUW + v90m / xd2gNNWQjrLhVoQPR

```
TUIZ3Ph1WVaj + ahJefivDrkRoHy3au000LYmYjgahwz46P0u05B / B5EqHdZ + XIWD
mbA4CD / pXvk1B + TJYm5Xf6dQlfe6yJvmjqIBxdZmv3lh8zwc4bmCXF2gw + nYSL0Z
ohEUGW6yhhtoPkg3Goi3XZZenMfvJ2II4pEZXNLxId26F0KCl3GBUzGpn / Z9Yr9y
4aOTHcyKJloJONDO1w2AFrR4pTqHTI2KpdVGI / IsELm8VCLAABpQ570su9t + Oza
8eOx79 + Rj1QqCyXBjhnEUhAFZdWCEOrCMc0u
-----END CERTIFICATE-----
```

Anonymous Call Home

Anonymous Call Home 機能は、Cisco がインベントリおよびテレメトリメッセージを匿名で受信できるようにする Smart Call Home 機能のサブ機能です。この機能を有効にして、識別情報を匿名のままにします。

匿名 Call Home の特徴は、次のとおりです。

- Unified Communications Manager は Smart Call Home バックエンドにインベントリおよびテレメトリメッセージのみを送信し、診断および設定情報は送信しません。
- また、ユーザに関する情報を送信しません（登録デバイスやアップグレード履歴など）。
- 匿名 Call Home オプションは、Cisco の Smart Call Home 機能への登録または権限付与を必要としません。
- インベントリおよびテレメトリメッセージは、Call Home バックエンドに定期的に（毎月1日）送信されます。
- Cisco Unified Communications Manager が匿名 Call Home を使用するように設定されている場合、トレースログと診断情報を含める オプションは無効になります。

インベントリメッセージには、クラスタ、ノード、ライセンスに関する情報が含まれます。

次の表に、Smart Call Home および Anonymous Call Home のインベントリメッセージを示します。

表 14: Smart Call Home および Anonymous Call Home のインベントリメッセージ

インベントリメッセージ	Smart Call Home	Anonymous Call Home
連絡先の電子メール	IOS-XRイメージに	N/A
連絡先電話番号（Contact Phone Number）	IOS-XRイメージに	N/A
組織の番地（Street Address）	IOS-XRイメージに	N/A
サーバ名	IOS-XRイメージに	N/A
サーバIPアドレス	IOS-XRイメージに	N/A

インベントリ メッセージ	Smart Call Home	Anonymous Call Home
ライセンスサーバ	IOS-XRイメージに	N/A
OS Version	適用可能	適用可能
Model	適用可能	適用可能
シリアル番号	適用可能	適用可能
CPU 速度	適用可能	適用可能
RAM	適用可能	適用可能
ストレージのパーティション (Storage Partition)	適用可能	適用可能
ファームウェアのバージョン	適用可能	適用可能
BIOS Version	適用可能	適用可能
BIOS 情報	適用可能	適用可能
RAID 設定 (Raid Configuration)	適用可能	適用可能
[Active Services]	適用可能	適用可能
[Publisher Name]	IOS-XRイメージに	N/A
パブリッシャ IP	IOS-XRイメージに	N/A
製品 ID	適用可能	適用可能
Active Version	適用可能	適用可能
Inactive Version	適用可能	適用可能
製品の略称 (Product Short name)	適用可能	適用可能

テレメトリ メッセージには、Unified Communications Manager クラスタで使用できる各デバイス タイプのデバイス数 (IP 電話、ゲートウェイ、会議ブリッジなど) に関する情報が含まれます。テレメトリ データには、クラスタ全体のデバイスの数が含まれます。

次の表に、Smart Call Home および Anonymous Call Home のテレメトリメッセージを示します。

表 15: Smart Call Home および Anonymous Call Home のテレメトリメッセージ

テレメトリ メッセージ	Smart Call Home	Anonymous Call Home
連絡先の電子メール	IOS-XRイメージに	N/A

テレメトリ メッセージ	Smart Call Home	Anonymous Call Home
連絡先電話番号 (Contact Phone Number)	IOS-XRイメージに	N/A
組織の番地 (Street Address)	IOS-XRイメージに	N/A
サーバ名	IOS-XRイメージに	N/A
CM ユーザ数 (CM User Count)	IOS-XRイメージに	N/A
シリアル番号	適用可能	適用可能
パブリッシャ名 (Publisher name)	IOS-XRイメージに	N/A
デバイス数とモデル	適用可能	適用可能
電話ユーザの数 (Phone User Count)	適用可能	適用可能
CM コールアクティビティ	適用可能	適用可能
登録されたデバイスの数 (Registered Device count)	IOS-XRイメージに	N/A
アップグレードの履歴 (Upgrade history)	IOS-XRイメージに	N/A
システム ステータス (System Status)	ホスト名、日付、ロケール、製品バージョン、OS バージョン、ライセンス MAC、アップタイム、MP Stat、使用されたメモリ、ディスク使用率、使用されているアクティブおよび非アクティブなパーティション、および DNS に適用されます。	日付、ロケール、製品バージョン、OS バージョン、ライセンス MAC、稼働時間、使用されたメモリ、ディスク使用率、および使用されているアクティブおよび非アクティブパーティションに適用されます。

設定メッセージには、設定に関連する各データベーステーブルの行カウントに関する情報が含まれています。この設定データはクラスタ全体の各テーブルのテーブル名と行数で構成されます。

Smart Call Home による処理

Cisco Systems と直接サービス契約を結んでいる場合は、Cisco Smart Call Home サービスに Unified Communications Manager を登録することができます。Smart Call Home は、Unified Communications Manager から送信された Call Home メッセージを分析し、背景情報および推奨事項を提供して、システムの問題を迅速に解決します。

Cisco Unified CM Call Home 機能は、Smart Call Home バック エンド サーバに次のメッセージを送信します。

- アラート：環境、ハードウェア障害、システムパフォーマンスに関連するさまざまな状況のアラート情報が含まれています。アラートは、Unified Communications Manager クラスタ内の任意のノードから生成される場合があります。アラートの詳細には、アラートのタイプに応じて、トラブルシューティングに必要なノードなどの情報が含まれています。Smart Call Home バックエンドサーバに送信されるアラートについては、Smart Call Home による処理に関するトピックを参照してください。

次に、Smart Call Home のアラートを示します。

デフォルトでは、Smart Call Home はアラートを24時間に1回処理します。混在クラスタ (Unified Communication Manager および Cisco Unified Presence) で 24 時間以内に同じアラートが繰り返し発生した場合は、Smart Call Home は処理を行いません。



重要 収集された情報は、48 年後にプライマリ AMC サーバから削除されます。デフォルトでは、Unified Communications Manager パブリッシャがプライマリ AMC サーバとなります。

- パフォーマンスに関連するアラート
 - CallProcessingNodeCPUpeging
 - CodeYellow
 - CPUpeging
 - LowActivePartitionAvailableDiskSpace
 - LowAvailableVirtualMemory
 - LowSwapPartitionAvailableDiskSpace
- データベースに関連するアラート
 - DBReplicationFailure
- 失敗したコールに関連するアラート
 - MediaListExhausted
 - RouteListExhausted
- クラッシュに関連するアラート
 - CoreDumpfilefound
 - CriticalServiceDown

設定、インベントリ、およびテレメトリメッセージは、Call Home バックエンドに定期的に(毎月1日)送信されます。これらのメッセージの情報を活用することで、TAC はお客様がネットワークを維持管理する上で役立つサービスをタイムリーかつ予防的に提供します。

Call Home の前提条件

Unified Communications Manager Call Home サービスをサポートするには、以下が必要となります。

- 対応する Unified Communications Manager サービス契約に関連付けられた Cisco.com ユーザ ID。
- ドメイン ネーム システム (DNS) と Simple Mail Transfer Protocol (SMTP) の両サーバを Unified Communications Manager Call Home 機能用に設定することを推奨します。
 - DNS 設定は、セキュア Web (HTTPS) を使用して Call Home メッセージを送信するために必要です。
 - SMTP セットアップは、Call Home メッセージを Cisco TAC に送信したり、電子メールで受信者のリストにメッセージのコピーを送信したりするために必要です。

Call Home へのアクセス

Unified CM Call Home にアクセスするには、Cisco Unified Serviceability 管理を開き、**CallHome (Cisco Unified Serviceability > CallHome > Call Home の設定)** を選択します。

Call Home の設定

以下の表は、Unified Communications Manager Call Home のデフォルト設定の一覧です。

表 16: Call Home のデフォルト設定

パラメータ	デフォルト
Call Home	有効 (Enabled)
Send Data to Cisco Technical Assistance Center (TAC) using	セキュア Web (HTTPS)

インストール時にデフォルトの Smart Call Home 設定が変更された場合は、Call Home ユーザーインターフェイスに同じ設定が反映されます。



- (注) 転送方式として [電子メール (Email)] を選択し、[smtp 設定 (smtp setup)] を [セキュア Web (HTTPS) (SECURE Web (HTTPS))] オプションにする必要がない場合は、smtp を設定する必要があります。

Call Home の設定

Cisco Unified Serviceability で、[Call Home]> [Call Home の設定 (Call Home Configuration)] を選択します。

[Call Home の設定 (Call Home Configuration)] ウィンドウが表示されます。



- (注) Unified Communications Manager のインストール時に Cisco Smart Call Home を設定することもできます。

Smart Call Home 機能は、インストール時に Smart Call Home オプションを設定すると有効になります。なしを選択すると、通知メッセージは Cisco Unified Communications Manager 管理にログインする際に表示されます。Smart Call Home を設定するか、Cisco Unified Serviceability を使用してリマインダを無効にする手順が表示されます。

次の表では、Cisco Unified Communications Manager Call Home の設定について説明しています。

表 17: Unified Communications Manager Call Home の設定の構成

フィールド名	説明
Call Home メッセージスケジュール (Call Home Message Schedule)	最後に送信された Call Home メッセージと、スケジュール設定されている次のメッセージの日付と時刻を表示します。

フィールド名	説明
Call Home*	<p>ドロップダウンリストから、次のいずれかのオプションを選択します。</p> <ul style="list-style-type: none"> • なし : Call Home を有効または無効にする場合は、このオプションを選択します。Smart Call Home が設定されていません、という再通知が表示されます。Smart Call Home の設定、あるいは再通知を無効にするには、[Cisco Unified Serviceability > Call Home] を開くか、管理者ページで、ここをクリックします。 • 無効 : Call Home を無効にする場合に、このオプションを選択します。 • 有効 (Smart Call Home) : インストール中に Smart Call Home を選択した場合は、このオプションが有効となります。このオプションを選択すると、[カスタマーの連絡先詳細 (Customer Contact Details)] の下のすべてのフィールドが有効になります。同じ設定では、[データの送信 (Send Data)] のオプションも有効になっています。 • 有効 (匿名 Call Home) : 匿名モードで Call Home を使用する場合には、このオプションを選択します。このオプションを選択すると、[カスタマーの連絡先詳細 (Customer Contact Details)] の下のすべてのフィールドが無効になります。同じ設定では、[データの送信 (Send Data)] で [次の電子メールアドレスにコピーを送信し (複数のアドレスをカンマで区切る) (Send a copy to the following email addresses (separate multiple addresses with comma))]、[データの送信 (Send Data)] フィールドが有効になっており、トレースログと診断情報は Call Home ページで無効になっています。 <p>(注) Anonymous Call Home を有効にすると、サーバはサーバから Cisco systems に使用状況の統計情報を送信します。この情報は、シスコが製品に関するユーザの体験を理解し、製品の方向を促進するのに役に立ちます。</p>
お客様の連絡先の詳細	
電子メール アドレス*	顧客の連絡先の電子メールアドレスを入力します。これは必須フィールドです。
企業名	(任意) 会社名を入力します。入力できるのは最大 255 文字です。

フィールド名	説明
連絡先の名前	任意顧客の連絡先の名前を入力します。最大 128 文字を入力できます。 担当者には、英数字とドット (.)、下線 (_)、ハイフン (-) などの一部の特殊文字を使用できます。
アドレス	(任意) 顧客の住所を入力します。入力できるのは最大 1024 文字です。
電話	(任意) 顧客の電話番号を入力します。
送信データ	
次を使用して Cisco Technical Assistance Center (TAC) にデータを送信 (Send Data to Cisco Technical Assistance Center (TAC) using)	これは必須フィールドです。ドロップダウンリストから、次のいずれかのオプションを選択して Call Home メッセージを Cisco TAC に送信します。 <ul style="list-style-type: none"> • セキュア Web (HTTPS) : セキュア Web を使用して Cisco TAC にデータを送信する場合は、このオプションを選択します。 • 電子メール : 電子メールを使用して Cisco TAC にデータを送信する場合は、このオプションを選択します。電子メールの場合は、SMTP サーバを設定する必要があります。設定されている SMTP サーバのホスト名または IP アドレスを確認できます。 (注) SMTP サーバを設定していない場合は、警告メッセージが表示されます。 • [プロキシ経由のセキュア Web (HTTPS) (Secure Web (HTTPS) through Proxy)] : プロキシ経由で Cisco TAC にデータを送信する場合には、このオプションを選択します。現在、プロキシレベルでの認証はサポートされていません。このオプションの設定には、次のフィールドが表示されます。 <ul style="list-style-type: none"> • HTTPS プロキシ IP または ホスト名*: プロキシの IP あるいはホスト名を入力します。 • HTTPS プロキシポート (HTTPS Proxy port) *: 通信するプロキシポート番号を入力します。
次の電子メールアドレスにコピーを送信します(複数のアドレスはカンマで区切ります)。	指定した電子メールアドレスに Call Home メッセージのコピーを送信するには、このチェックボックスをオンにします。最大 1024 文字まで入力できます。

フィールド名	説明
トレースログと診断情報を含める (Include Trace logs and Diagnostics Information)	<p>Cisco Unified CM のログおよび診断情報の収集を有効にするには、このチェック ボックスをオンにします。</p> <p>(注) このオプションは、Smart Call Home が有効になっている場合にのみアクティブになります。</p> <p>メッセージには、アラート時に収集された診断情報とともに、トレースメッセージが含まれています。トレースサイズが 3 MB 未満の場合、トレースはエンコードされ、アラートメッセージの一部として送信されます。トレースが 3 MB を超えると、トレースの場所のパスがアラートメッセージに表示されます。</p>
保存 (Save)	<p>Call Home 設定を保存します。</p> <p>(注) Call Home 設定を保存すると、エンドユーザライセンス契約 (EULA) のメッセージが表示されます。初めて設定する場合は、ライセンス契約に同意する必要があります。</p> <p>ヒント アクティブ化した Call Home サービスを非アクティブ化するには、ドロップダウンリストから [無効 (Disabled)] オプションを選択し、[保存 (Save)] をクリックします。</p>
リセット	最後に保存された設定にリセットします。
保存して今すぐ Call Home を送信 (Save and Call Home Now)	<p>Call Home メッセージを保存して送信します。</p> <p>(注) メッセージが正常に送信されると、Call home の設定が保存され、すべての Call Home メッセージが正常に送信されます。</p>

制限事項

Unified Communications Manager サーバ あるいは Cisco Unified Presence サーバがダウンしている場合、または接続不能である場合には、以下の制限事項が適用されます。

- Smart Call Home は、サーバが到達可能になるまで、送信された最後の Call Home メッセージおよびスケジュール設定されている次のメッセージの日時をキャプチャできません。
- Smart Call Home は、サーバが到達可能になるまで Call Home メッセージを送信しません。
- パブリッシャがダウンしている場合、Smart Call Home はインベントリメール内のライセンス情報をキャプチャできません。

次の制限は、Alert Manager と Collector (AMC) によるものです。

- ノード A でアラートが発生し、プライマリ AMC サーバ(デフォルトではパブリッシャ)が再起動され、同じアラートが同じノードで24時間の間に発生した場合、Smart Call Home はノード A からアラートデータを再送信します。Smart Call Home は **alre** があるアラートを認識できません。プライマリ AMC が再起動されたため、**ady** が発生しました。
- ノード A でアラートが発生し、プライマリ AMC サーバを別のノードに変更した場合、および同じノードで24時間の間に同じアラートが発生した場合、Smart Call Home はノード A の新しいアラートとして認識し、アラートデータを送信します。
- プライマリ AMC サーバで収集されたトレースは、いくつかのシナリオで、プライマリ AMC サーバに存在する可能性があり、最大60時間です。

混在クラスタ（Cisco Unified Communications Manager および IM and Presence）シナリオにおける制限事項は以下の通りです。

- **CallProcessingNodeCpuPegging**、メディアリストの枯渇、ルートリストの枯渇などのアラートは、IM and Presence には適用されません。
- ユーザがプライマリ AMC サーバを IM and Presence に変更した場合、Smart Call Home は、メディアリストが使い果たされ、ルートリストが枯渇した場合に、cluster の概要レポートを生成できません。
- ユーザがプライマリ AMC サーバを IM and Presence に変更した場合、Smart Call Home は **DB レプリケーション**アラートの概要レポートを生成できません。

Call Home の参照先

Smart Call Home の詳細については、次の URL を参照してください。

- Smart Call Home サービスの概要
http://www.cisco.com/en/US/products/ps7334/serv_home.html



第 14 章

Serviceability Connector

- [Serviceability Connector の概要 \(169 ページ\)](#)
- [Serviceability サービスを使用する利点 \(170 ページ\)](#)
- [他のハイブリッドサービスとの違い \(170 ページ\)](#)
- [動作の簡単な説明 \(170 ページ\)](#)
- [TAC ケースの展開アーキテクチャ \(171 ページ\)](#)
- [Serviceability Connector の TAC サポート \(173 ページ\)](#)

Serviceability Connector の概要

Webex Serviceability サービスを使用すると、ログの収集を容易にすることができます。このサービスでは、診断ログと情報を検索、取得して、タスクを自動化します。

この機能は、オンプレミスで導入された有用性コネクタを使用します。有用性コネクタは、ネットワーク内の専用のネットワーク(「コネクタホスト」)で実行されます。コネクタは、次のいずれかのコンポーネントに取り付けることができます。

- エンタープライズ コンピューティング プラットフォーム (ECP) - 推奨

ECPは、**Docker** コンテナを使用して、サービスを分離、保護、および管理します。ホストと有用性コネクタアプリケーションはクラウドからインストールされます。最新かつ安全な状態を維持するために、手動でアップグレードする必要はありません。



重要 ECPの使用を推奨します。私たちの将来の開発は、このプラットフォームに焦点を当てます。Expresswayに有用性コネクタをインストールすると、一部の新機能が使用できなくなります。

- Cisco Expressway

次の目的で有用性コネクタを使用できます。

- サービスリクエストの自動ログおよびシステム情報取得
- クラウドに接続されている UC 展開での Unified CM クラスタのログ収集

両方のユースケースで同じ有用性コネクタを使用できます。

Serviceability サービスを使用する利点

このサービスには次の利点があります。

- ログの収集を高速化します。TACエンジニアは、問題の診断を実行する際に関連するログを取得できます。追加のログを要求し、手動での収集と配信を待機する遅延を回避できます。この自動化により、問題解決にかかる時間を数日にすることができます。
- TAC の Collaboration Solution Analyzer および診断シングニチャのデータベースと連携します。システムは自動的にログを分析し、既知の問題を特定して、既知の修正または回避策を推奨します。

他のハイブリッドサービスとの違い

ハイブリッドカレンダーサービスやハイブリッドコールサービスなどの他のサーバと同様の方法で、制御ハブを使用して有用性コネクタを展開および管理できます。ただし、重要な違いがあります。

このサービスには、ユーザ向けの機能はありません。TACは、このサービスの主要なユーザです。他のハイブリッドサービスを使用する組織にはメリットがありますが、他のハイブリッドサービスを使用しない組織が一般的なユーザです。

すでに組織がコントロールハブで設定されている場合は、既存の組織の管理者アカウントを使用してサービスを有効にすることができます。

有用性コネクタには、ユーザに直接機能を提供するコネクタとは異なるロードプロファイルがあります。コネクタは常に使用可能であるため、TACは必要に応じてデータを収集できます。ただし、時間の経過とともに安定したロードになるわけではありません。TAC担当者が手動でデータ収集を開始します。担当者は同じインフラストラクチャによって提供される他のサービスへの影響を最小限に抑えるために、適切な時間をネゴシエートします。

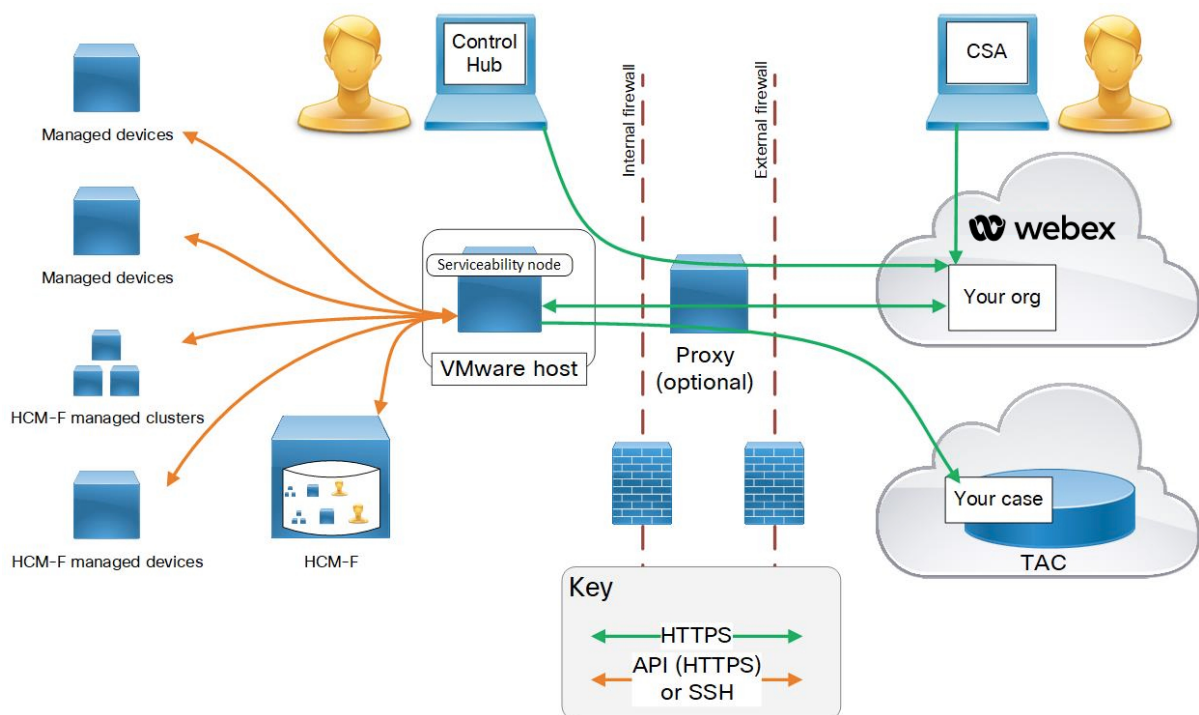
動作の簡単な説明

1. 管理者は、Cisco TAC と連携して、有用性サービスを導入します。[TAC ケースの展開アーキテクチャ \(171 ページ\)](#) を参照してください。
2. TACは、いずれかのシスコデバイス(ケースをオープンした場合した場合)の問題を学習します。
3. TACの担当者は、コラボレーションソリューションアナライザ(CSA)のWebインターフェイスを使用して、関連するデバイスからデータを収集するための有用性コネクタを要求します。

4. 有用性コネクタは、管理対象デバイスから要求されたデータを収集するために、API コマンドに要求を変換します。
5. 有用性コネクタは、カスタマー エクスペリエンス ドライブ (CXD) への暗号化されたリンクを介してそのデータを収集、暗号化、およびアップロードし、サービスリクエストにデータを関連付けます。
6. データは、1000を超える診断シグニチャの TAC データベースに対して分析します。
7. TAC 担当者が結果を確認し、必要に応じてオリジナルのログを確認します。

TAC ケースの展開アーキテクチャ

図 3: *Expressway* でのサービス コネクタを使用した展開



要素	説明
管理対象デバイス	<p>有用性サービスにログを提供するデバイスが含まれます。1つの有用性コネクタを使用して、最大150のローカル管理デバイスを追加できます。HCSのお客様の管理対象デバイスおよびクラスタ（デバイスの数が多い場合は https://help.webex.com/en-us/142g9e/Limits-and-Bounds-of-Serviceability-Service を参照）に関する情報を HCM-F（Hosted Collaboration Mediation Fulfillment）からインポートできます。</p> <p>サービスは現在、次のデバイスと連携しています。</p> <ul style="list-style-type: none"> • Hosted Collaboration Mediation Fulfillment (HCM-F) • Cisco Unified Communications Manager • Cisco Unified CM IM and Presence サービス • Cisco Expressway シリーズ • Cisco TelePresence Video Communication Server (VCS) • Cisco Unified Contact Center Express (UCCX) • Cisco Unified Border Element (CUBE) • Cisco BroadWorks アプリケーションサーバ (AS) • Cisco BroadWorks Profile Server (PS) • Cisco BroadWorks Messaging Server (UMS) • Cisco BroadWorks Execution Server (XS) • Cisco Broadworks Xtended Services Platform (XSP)
管理者	<p>Control Hub を使用してコネクタホストを登録し、有用性サービスを有効にします。URLはhttps://admin.webex.comであり、「組織管理者」のクレデンシャルが必要です。</p>
コネクタホスト	<p>管理コネクタと有用性コネクタをホストする Enterprise Compute Platform (ECP) または Expressway。</p> <ul style="list-style-type: none"> • 管理コネクタ（ECP または Expressway 上）および対応する管理サービス（Webex 内）が登録を管理します。接続を維持し、必要に応じてコネクタを更新して、ステータスとアラームを報告します。 • 有用性コネクタ：組織で有用性サービスを有効にした後、コネクタホスト（ECP または Expressway）が Webex からダウンロードする小さいアプリケーション。

要素	説明
[プロキシ (Proxy)]	(オプション) 有用性コネクタを起動した後にプロキシ設定を変更した場合は、有用性コネクタを再起動する必要があります。
Webex クラウド	Webex、Webex Calling、Webex Meetings、および Webex ハイブリッドサービスをホストします。
テクニカルアシスタンスセンター	内容： <ul style="list-style-type: none">• CSA を使用して、Webex Cloud 経由で有用性コネクタと通信する TAC の担当者。• ケースと、有用性コネクタによって収集された関連ログを使用した TAC ケース管理システム。

Serviceability Connector の TAC サポート

有用性コネクタの詳細については<https://www.cisco.com/go/serviceability>、を参照するか、TAC の担当者にお問い合わせください。



第 15 章

簡易ネットワーク管理プロトコル

- 簡易ネットワーク管理プロトコル (SNMP) のサポート (175 ページ)
- SNMP 設定タスク フロー (200 ページ)
- SNMP トラップ設定 (SNMP Trap Settings) (218 ページ)
- SNMP トレースの設定 (222 ページ)
- SNMP のトラブルシューティング (222 ページ)

簡易ネットワーク管理プロトコル (SNMP) のサポート

アプリケーション層プロトコルである SNMP を使用すると、ノードやルータなどのネットワーク デバイス間の管理情報を簡単に交換できます。TCP/IP プロトコルスイートの一部である SNMP を使用すると、管理者はリモートでネットワークのパフォーマンスを管理し、ネットワークの問題を検出および解決し、ネットワークの拡張計画を立てることができます。

Serviceability GUI を使用して、V1、V2c、および V3 のコミュニティストリング、ユーザ、通知先など、SNMP 関連の設定を行います。設定した SNMP 設定は、ローカルノードに適用されます。ただし、システム設定でクラスタがサポートされている場合は、[SNMP 設定 (SNMP configuration)] ウィンドウの [「すべてのノードに適用 (apply To All Nodes) 」] オプションを使用して、クラスタ内のすべてのサーバに設定を適用できます。



ヒント Unified Communications Manager のみ : Cisco Unified CallManager または Unified Communications Manager 4.X で指定した SNMP 設定パラメータは、Unified Communications Manager 6.0 以降のアップグレード時に移行されません。シスコのユニファイドサービスでは、SNMP の設定手順を再度実行する必要があります。

SNMP は IPv4 と IPv6 をサポートし、CISCO-CCM-MIB には IPv4 と IPv6 の両方のアドレスやプリファレンスなどの列とストレージが含まれています。

SNMP の基礎

SNMP 管理のネットワークは、管理対象デバイス、エージェント、およびネットワーク管理システムという 3 つの主要コンポーネントで構成されています。

- 管理対象デバイス：SNMP エージェントを含み、管理対象ネットワークに存在するネットワーク ノード。管理対象デバイスには管理情報が収集および格納され、その情報は SNMP を使用することによって利用可能になります。

Unified Communications Manager および IM and Presence サービスのみ: クラスタをサポートする設定では、クラスタ内の最初のノードが管理対象デバイスとして機能します。

- エージェント：管理対象デバイスに存在するネットワーク管理対象ソフトウェアモジュール。エージェントには、管理情報のローカルな知識が蓄積され、SNMP と互換性のある形式に変換されます。

SNMP をサポートするため、マスターエージェントとサブエージェントのコンポーネントが使用されます。マスター エージェントはエージェント プロトコル エンジンとして機能し、SNMP 要求に関連する認証、許可、アクセスコントロール、およびプライバシーの機能を実行します。同様に、マスター エージェントには、MIB-II に関係するいくつかの管理情報ベース (MIB) 変数が含まれています。また、マスターエージェントは、サブエージェントへの接続も行います。サブエージェントでの必要なタスクが完了すると、その接続を解除します。SNMP マスターエージェントはポート 161 で待ち受けし、ベンダー MIB の SNMP パケットを転送します。

Unified Communications Manager サブ エージェントは、ローカルの Unified Communications Manager のみと通信します。Unified Communications Manager サブエージェントは SNMP マスター エージェントにトラップと情報メッセージを送信し、SNMP マスター エージェントは SNMP トラップ レシーバ (通知の宛先) と通信します。

IM and Presence Service サブエージェントは、ローカルの IM and Presence Service とのみ対話します。IM and Presence Service サブエージェントは SNMP マスター エージェントにトラップと情報メッセージを送信し、SNMP マスター エージェントは SNMP トラップ レシーバ (通知の宛先) と通信します。

- ネットワーク管理システム (NMS)：SNMP 管理アプリケーション (および動作する PC)。ネットワーク管理に必要な処理リソースとメモリ リソースのほとんどを提供します。NMS では、管理対象デバイスをモニタおよび制御するアプリケーションが実行されます。次の Nms がサポートされています。
 - CiscoWorks LAN Management Solution (LMS)
 - HP OpenView
 - SNMP および Unified Communications Manager SNMP インターフェイスをサポートするサードパーティ製アプリケーション

SNMP 管理情報ベース

SNMP では、階層的に編成された情報のコレクションである管理情報ベース (MIB) にアクセスできます。MIB は、オブジェクト ID で識別される管理対象オブジェクトで構成されます。MIB オブジェクトには、管理対象デバイスの特定の特性が格納され、1つ以上のオブジェクトインスタンス (変数) で構成されます。

SNMP インターフェイスでは、次のシスコ標準 MIB が提供されます。

- CISCO-CDP-MIB
- CISCO-CCM-MIB
- CISCO-SYSLOG-MIB
- CISCO-UNITY-MIB

次の制限事項があります。

- Unified Communications Manager は、CISCO-UNITY-MIB をサポートしていません。
- Cisco Unity Connection では CISCO-CCM-MIB はサポートされません。
- IM and Presence Service では CISCO-CCM-MIB および CISCO-UNITY-MIB はサポートされません。

SNMP 拡張エージェントはサーバに常駐し、サーバが認識しているデバイスに関する詳細情報を提供する CISCO-CCM-MIB を公開します。クラスタ構成の場合、SNMP 拡張エージェントはクラスタ内の各サーバに常駐します。CISCO-CCM-MIB は、サーバ (クラスタでなく、クラスタをサポートする構成内のサーバ) にデバイスの登録状態、IP アドレス、説明、およびモデルタイプなどのデバイス情報を提供します。

SNMP インターフェイスでは、次の業界標準 MIB も提供されます。

- SYSAPPL-MIB
- MIB-II (RFC 1213)
- HOST-RESOURCES-MIB

CISCO-CDP-MIB

Cisco Discovery Protocol MIB (CISCO-CDP-MIB) を読み取るには、CDP サブエージェントを使用します。この MIB を使用すると、SNMP 管理対象デバイスが自身をネットワーク上の他のシスコ デバイスにアダプタイズできるようになります。

CDP サブエージェントは CDP-MIB を実装します。CDP-MIB には、次のオブジェクトが含まれています。

- cdpInterfaceIfIndex
- cdpInterfaceMessageInterval
- cdpInterfaceEnable

- cdpInterfaceGroup
- cdpInterfacePort
- cdpGlobalRun
- cdpGlobalMessageInterval
- cdpGlobalHoldTime
- cdpGlobalLastChange
- cdpGlobalDeviceId
- cdpGlobalDeviceIdFormat
- cdpGlobalDeviceIdFormatCpd



(注) CISCO-CDP-MIB は、次の MIB の存在に依存しています。CISCO-SMI、CISCO-TC、CISCO-VTP-MIB。

SYSAPPL-MIB

インストールされているアプリケーション、アプリケーションコンポーネント、システム動作しているプロセスなど、SYSAPPL-MIB から情報を取得するには、System Application Agent を使用します。

System Application Agent は、SYSAPPL-MIB の次のオブジェクトグループをサポートしています。

- sysApplInstallPkg
- sysApplRun
- sysApplMap
- sysApplInstallElmt
- sysApplElmtRun

表 18: SYSAPPL-MIB のコマンド

コマンド	説明
デバイスに関連するクエリー	
sysApplInstallPkgVersion	ソフトウェアの製造元によってアプリケーションパッケージに割り当てられたバージョン番号を提供します。
sysApplElmPastRunUser	プロセス所有者のログイン名 (root など) を提供します。

メモリ、ストレージ、CPUに関連するクエリー	
sysAppElmPastRunMemory	このプロセスが終了するまでに割り当てられた実システムメモリの合計 (KB 単位) の最新の既知の値を提供します。
sysAppElmtPastRunCPU	このプロセスによって消費されたシステムCPUリソースの合計 (1/100 秒単位) の最新の既知の値を提供します。 (注) マルチプロセッサ システムでは、この値は実際の時間 (実時間) の 1/100 秒よりも大きい単位で増加する可能性があります。
sysAppInstallElmtCurSizeLow	現在のファイルサイズ (modulo 2^{32} バイト) を提供します。たとえば、合計 4,294,967,296 バイトあるファイルに対して、この変数の値は 0 になります。4,294,967,295 バイトあるファイルに対して、変数の値は 4,294,967,295 になります。
sysAppInstallElmtSizeLow	インストールされたファイルサイズ (modulo 2^{32} バイト) を提供します。これは、インストール直後のディスク上のファイルのサイズです。たとえば、合計 4,294,967,296 バイトあるファイルに対して、この変数の値は 0 になります。4,294,967,295 バイトあるファイルに対して、変数の値は 4,294,967,295 になります。
sysAppElmRunMemory	このプロセスに現在割り当てられている実システムメモリの合計値 (KB 単位) を提供します。
sysAppElmRunCPU	このプロセスによって消費されたシステムCPUリソースの合計値 (1/100 秒単位) を提供します。 (注) マルチプロセッサ システムでは、この値は実際の時間 (実時間) の 1/100 秒よりも大きい単位で増加する可能性があります。

プロセスに関連するクエリー	
sysAppElmtRunState	実行中のプロセスの現在の状態を提供します。想定される値は実行中 (1)、実行可能 (2) ですが、CPU などのリソースの待ち状態の場合は、待機中 (3)、イベントの場合は、終了中 (4) またはその他 (5) になります。
sysAppElmtRunNumFiles	プロセスによって現在開かれている通常ファイルの数を提供します。この値の計算には、転送接続 (ソケット) や、オペレーティングシステム固有の特殊なファイルタイプは含まれません。
sysAppElmtRunTimeStarted	プロセスが開始された時刻を提供します。
sysAppElmtRunMemory	このプロセスに現在割り当てられている実システムメモリの合計値 (KB 単位) を提供します。
sysAppElmtPastRunInstallID	インストール済み要素テーブルのインデックスを提供します。このオブジェクトの値は、前回実行したプロセスを示すエントリのアプリケーションエレメントに対する sysAppInstallElmtIndex と同じです。
sysAppElmtPastRunUser	プロセス所有者のログイン名 (root など) を提供します。
sysAppElmtPastRunTimeEnded	プロセスが終了した時刻を提供します。
sysAppElmtRunUser	プロセス所有者のログイン名 (root など) を提供します。
sysAppRunStarted	アプリケーションが起動された日時を提供します。

sysAppElmtRunCPU	このプロセスによって消費されたシステム CPU リソースの合計値 (1/100 秒単位) を提供します。 (注) マルチプロセッサ システムでは、この値は実際の時間 (実時間) の 1/100 秒よりも大きい単位で増加する可能性があります。
ソフトウェア コンポーネントに関連するクエリー	
sysAppInstallPkgProductName	製造元によってソフトウェア アプリケーション パッケージに割り当てられた名前を提供します。
sysAppElmtRunParameters	プロセスの起動パラメータを提供します。
sysAppElmtRunName	プロセスのフルパスとファイル名を提供します。たとえば、実行パスが「opt/MYYpkg/bin/myyproc」のプロセス「myyproc」の場合は「/opt/MYYpkg/bin/myyproc」が返されます。
sysAppInstallElmtName	アプリケーションに含まれるこの要素の名前を提供します。
sysAppElmtRunUser	プロセス所有者のログイン名 (root など) を提供します。

sysApplInstallElmtPath	<p>この要素がインストールされているディレクトリのフルパスを提供します。たとえば、「/opt/EMPuma/bin」ディレクトリにインストールされている要素の場合、値は「/opt/EMPuma/bin」になります。ほとんどのアプリケーションパッケージには、パッケージ内の要素に関する情報が含まれています。また、要素は通常、パッケージのインストールディレクトリのサブディレクトリにインストールされます。パッケージの情報自体に要素のパス名が含まれていない場合、通常はサブディレクトリの簡易検索でパスを特定することができます。要素がその場所にインストールされておらず、エージェント実装のために別の情報も参照できない場合には、パスは不明となり、null が返されます。</p>
sysApplMapInstallPkgIndex	<p>このオブジェクトの値を提供し、このプロセスが含まれているアプリケーションのインストール済みソフトウェアパッケージを特定します。プロセスの親アプリケーションを特定できる場合、このオブジェクトの値は、このプロセスが含まれているインストール済みアプリケーションに対応する sysApplInstallPkgTable のエントリの sysApplInstallPkgIndex と同じになります。ただし、親アプリケーションを特定できない場合には（プロセスが特定のインストール済みアプリケーションに含まれない場合など）、このオブジェクトの値は「0」になります。これは、このプロセスをアプリケーションやインストール済みソフトウェアパッケージと関連付けることができないことを示します。</p>

sysApplElmtRunInstallID	sysApplInstallElmtTable のインデックスを提供します。このオブジェクトの値は、実行中のインスタンスを示すエントリのアプリケーションエレメントに対する sysApplInstallElmtIndex と同じです。このプロセスをインストール済みで実行可能なプロセスと関連付けることができない場合、値は「0」になります。
sysApplRunCurrentState	実行中のアプリケーション インスタンスの現在の状態を提供します。想定される値は実行中 (1)、実行可能 (2) ですが、CPU などのリソースの待ち状態の場合は、待機中 (3)、イベントの場合は、終了中 (4) またはその他 (5) になります。この値は、このアプリケーションインスタンス (sysApplElmRunState を参照) の実行中のエレメントの評価をもとにしており、ロールは sysApplInstallElmtRole で定義されています。エージェントの導入で、「必須」の複数のエレメントが実行できなくなった場合、アプリケーションインスタンスが終了中のプロセスにあるかを検出できます。エージェント実装のほとんどは、システム時刻を提供して REQUIRED 要素を開始するために、2 番目の内部ポーリングが完了するまで待機してからアプリケーションインスタンスを終了としてマークします。
sysApplInstallPkgDate	このソフトウェア アプリケーションがホストにインストールされた日時を提供します。
sysApplInstallPkgVersion	ソフトウェアの製造元によってアプリケーション パッケージに割り当てられたバージョン番号を提供します。
sysApplInstallElmtType	インストール済みアプリケーションに含まれている要素のタイプを提供します。
日付または時刻に関連するクエリー	

sysApplElmtRunCPU	このプロセスによって消費されたシステム CPU リソースの合計値 (1/100 秒単位) です。 (注) マルチプロセッサ システムでは、この値は実際の時間 (実時間) の 1/100 秒よりも大きい単位で増加する可能性があります。
sysApplInstallPkgDate	このソフトウェア アプリケーションがホストにインストールされた日時を提供します。
sysApplElmtPastRunTimeEnded	プロセスが終了した時刻を提供します。
sysApplRunStarted	アプリケーションが起動された日時を提供します。

MIB-II

MIB-II から情報を取得するには、MIB2 エージェントを使用します。MIB2 エージェントは、インターフェイスや IP など、RFC 1213 で定義されている変数へのアクセスを提供し、次のオブジェクト グループをサポートしています。

- system
- interfaces
- at
- ip
- icmp
- tcp
- udp
- snmp

表 19: MIB-II コマンド

コマンド	説明
デバイスに関連するクエリー	
sysName	この管理対象ノードに管理上割り当てられた名前を提供します。慣例として、この名前はノードの完全修飾ドメイン名になります。名前が不明な場合、この値は長さがゼロの文字列になります。

sysDescr	エンティティの説明テキストを提供します。この値には、システムのハードウェアタイプ、ソフトウェアオペレーティングシステム、ネットワークソフトウェアの完全な名前とバージョン識別番号が含まれます。
SNMP 診断クエリー	
sysName	この管理対象ノードに管理上割り当てられた名前を提供します。慣例として、この名前はノードの完全修飾ドメイン名になります。名前が不明な場合、この値は長さがゼロの文字列になります。
sysUpTime	システムのネットワーク管理部分が最後に再初期化されてからの時間（1/100 秒単位）を提供します。
snmpInTotalReqVars	有効な SNMP Get-Request と Get-Next PDU を受信した結果として、SNMP プロトコルエンティティによって正常に取得された MIB オブジェクトの合計数を提供します。
snmpOutPkts	SNMP エンティティから転送サービスに渡された SNMP メッセージの合計数を提供します。

<p>sysServices</p>	<p>このエンティティが提供する可能性があるサービスのセットを示す値を提供します。The value is a sum. この合計は最初は 0 の値を取りますが、このノードがトランザクションを実行する各レイヤ (L) について 1 ~ 7 の範囲を取り、この合計に (L - 1) の 2 乗が加算されます。たとえば、アプリケーションサービスを提供するホストであるノードの値が $4 (2^{(3-1)})$ になる場合や、アプリケーションサービスを提供するホストのノードの値が $72 (2^{(4-1)} + 2^{(7-1)})$ になる場合があります。</p> <p>(注) プロトコルのインターネットスイートの場合には、レイヤ1の物理 (リピータなど)、レイヤ2のデータリンクまたはサブネットワーク (ブリッジなど)、レイヤ3のインターネット (IP をサポート)、レイヤ4のエンドツーエンド (TCP をサポート)、レイヤ7のアプリケーション (SMTP をサポート) を計算します。</p> <p>OSI プロトコルを含むシステムでは、レイヤ5および6も計算できます。</p>
<p>snmpEnableAuthenTraps</p>	<p>SNMP エンティティが authenticationFailure トラップの生成を許可されているかどうかを示します。このオブジェクトの値は、すべての設定情報を上書きします。そのため、すべての authenticationFailure トラップを無効化できる手段が提供されます。</p> <p>(注) シスコでは、このオブジェクトを不揮発性メモリに保存して、ネットワーク管理システムの再初期化後にも維持されるようにすることを強く推奨します。</p>
<p>Syslog に関連するクエリー</p>	

snmpEnabledAuthenTraps	<p>SNMP エンティティが authenticationFailure トラップの生成を許可されているかどうかを示します。このオブジェクトの値は、すべての設定情報を上書きします。そのため、すべての authenticationFailure トラップを無効化できる手段が提供されます。</p> <p>(注) シスコでは、このオブジェクトを不揮発性メモリに保存して、ネットワーク管理システムの再初期化後にも維持されるようにすることを強く推奨します。</p>
日付または時刻に関連するクエリー	
sysUpTime	<p>システムのネットワーク管理部分が最後に再初期化されてからの時間 (1/100 秒単位) を提供します。</p>

HOST-RESOURCES MIB

HOST-RESOURCES-MIB から値を取得するには、Host Resources Agent を使用します。Host Resources Agent は、ストレージリソース、プロセステーブル、デバイス情報、およびインストールされたソフトウェアベースなど、ホスト情報に対する SNMP アクセスを提供します。Host Resources Agent は次のオブジェクトグループをサポートしています。

- hrSystem
- hrStorage
- hrDevice
- hrSWRun
- hrSWRunPerf
- hrSWInstalled

表 20: HOST-RESOURCES MIB のコマンド

コマンド	説明
デバイスに関連するクエリー	
hrFSMountPoint	このファイルシステムのルートのパス名を提供します。
hrDeviceDescr	デバイスの製造元やリビジョン、シリアル番号 (オプション) など、このデバイスの説明テキストを提供します。

hrStorageDescr	ストレージのタイプおよびインスタンスの説明を提供します。
メモリ、ストレージ、CPU に関連するクエリー	
hrMemorySize	ホストに搭載されている物理的な読み取り/書き込みメインメモリ（通常は RAM）の容量を提供します。
hrStorageSize	ストレージのサイズを hrStorageAllocationUnits の単位で提供します。このオブジェクトは書き込み可能であるため、操作が理に適っており、基盤となるシステムで実行可能な場合には、ストレージエリアのサイズのリモート設定が可能です。たとえば、バッファプールに割り当てるメモリの量や、仮想メモリに割り当てるディスク容量を変更できます。
プロセスに関連するクエリー	
hrSWRunName	製造元、リビジョン、一般に知られている名前など、この実行中のソフトウェアの説明テキストを提供します。このソフトウェアがローカルにインストールされている場合は、対応する hrSWInstalledName で使用されているものと同じ文字列である必要があります。
hrSystemProcesses	このシステムに現在ロードされているか、実行中のプロセスコンテキストの数を提供します。
hrSWRunIndex	ホストで実行中の各ソフトウェアに固有の値を提供します。可能な限り、ネイティブかつ一意のシステム識別番号を使用します。
ソフトウェア コンポーネントに関連するクエリー	
hrSWInstalledName	製造元、リビジョン、一般に知られている名前、およびシリアル番号（オプション）など、このインストールされているソフトウェアの説明テキストを提供します。
hrSWRunPath	このソフトウェアのロード元である長期ストレージの場所（ディスクドライブなど）の説明を提供します。
日付または時刻に関連するクエリー	
hrSystemDate	ホストのローカルの日時を提供します。

hrFSLastPartialBackupDate	このファイルシステムの一部が、バックアップのために別のストレージデバイスにコピーされた最後の日付を提供します。この情報は、バックアップが定期的に行われているかを確認するのに役立ちます。この情報が不明な場合、この変数は 0000 年 1 月 1 日 00:00:00.0 に対応する値となり、「00 00 01 01 00 00 00 00」（16 進数）と符号化されます。
---------------------------	--

CISCO-SYSLOG-MIB

Syslog は、情報レベルから重大なものまでのすべてのシステムメッセージを追跡し、ログに記録します。この MIB を使用すると、ネットワーク管理アプリケーションでは Syslog メッセージを SNMP トラップとして受信できるようになります。

Cisco Syslog Agent では、次の MIB オブジェクトによるトラップ機能をサポートしています。

- clogNotificationsSent
- clogNotificationsEnabled
- clogMaxSeverity
- clogMsgIgnores
- clogMsgDrops



(注) CISCO-SYSLOG-MIB は、CISCO-SMI MIB の存在に依存します。

表 21 : CISCO-SYSLOG-MIB のコマンド

コマンド	説明
Syslog に関連するクエリー	
clogNotificationEnabled	デバイスが Syslog メッセージを生成するときに、clogMessageGenerated 通知が送信されるかどうかを示します。通知の無効化で syslog メッセージを clogHistoryTable に追加されることは中断されません。

clogMaxSeverity	<p>これは、どの syslog のシビラティ（重大度）レベルが実施されるかを示します。エージェントは、シビラティ（重大度）がこの値より大きい Syslog メッセージを無視します。</p> <p>(注) シビラティ（重大度）は数値が大きくなるほど低くなります。たとえば、エラー（4）は、デバッグ（8）よりシビラティ（重大度）が高いです。</p>
-----------------	---

CISCO-CCM-MIB および CISCO-CCM-CAPABILITY MIB

CISCO-CCM-MIB には、Unified Communications Manager と、Unified Communications Manager ノードで確認できる、電話やゲートウェイなどのそれに関連するデバイスについての動的な（リアルタイム）情報と設定された（静的）情報の両方が含まれています。簡易ネットワーク管理プロトコル（SNMP）テーブルには、IP アドレス、登録ステータス、およびモデルタイプなどの情報が格納されています。

SNMP は IPv4 と IPv6 をサポートし、CISCO-CCM-MIB には IPv4 と IPv6 の両方のアドレスやプリファレンスなどの列とストレージが含まれています。



- (注) Unified Communications Manager は、Unified Communications Manager システム内のこの MIB をサポートしています。IM and Presence Service と Cisco Unity Connection はこの MIB をサポートしていません。

CISCO-CCM-MIB および MIB 定義のサポートリストを参照するには、次のリンクにアクセスしてください。

<ftp://ftp.cisco.com/pub/mibs/supportlists/callmanager/callmanager-supportlist.html>

廃止オブジェクトを含め、Unified Communications Manager リリース全体での MIB の依存関係と MIB コンテンツを表示するには、次のリンクにアクセスしてください。 <http://tools.cisco.com/Support/SNMP/do/BrowseMIB.do?local=en&step=2&mibName=CISCO-CCM-CAPABILITY>

動的テーブルは、Cisco CallManager サービスが起動され、実行中の場合のみ入力されます（または Unified Communications Manager クラスタ設定の場合は、ローカルの Cisco CallManager サービス）。静的テーブルは、Cisco CallManager SNMP サービスが実行中の場合に入力されます。

表 22: Cisco-CCM-MIB の動的テーブル

テーブル	コンテンツ
ccmTable	このテーブルには、ローカル Unified Communications Manager のバージョンおよびインストール ID が保存されます。また、このテーブルには、ローカルの Unified Communications Manager が認識するクラスタ内のすべての Unified Communications Manager についての情報も保存されますが、バージョンの詳細は、「「unknown」」と示されます。ローカルの Unified Communications Manager がダウンした場合、バージョンおよびインストール ID の値を除き、テーブルは空のままになります。
ccmPhoneFailed、 ccmPhoneStatusUpdate、 ccmPhoneExtn、ccmPhone、 ccmPhoneExtension	Cisco Unified IP Phone の場合、ccmPhoneTable の登録済み電話機の数は、Unified Communications Manager/RegisteredHardware Phones perfmon カウンタと一致する必要があります。ccmPhoneTable には、登録済み、未登録、および拒否された Cisco Unified IP Phone ごとに 1 つのエントリがあります。ccmPhoneExtnTable では、インデックス ccmPhoneIndex と ccmPhoneExtnIndex を組み合わせて、ccmPhoneTable と ccmPhoneExtnTable のエントリが関連付けられます。
ccmCTIDevice、 ccmCTIDeviceDirNum	ccmCTIDeviceTable には、各 CTI デバイスが 1 つのデバイスとして保存されます。CTI ルートポイントまたは CTI ポートの登録ステータスに基づいて、Unified Communications Manager MIB 内の ccmRegisteredCTIDevices、ccmUnregisteredCTIDevices、ccmRejectedCTIDevices カウンタが更新されます。
ccmSIPDevice	CCMSIPDeviceTable には、各 SIP トランクが 1 つのデバイスとして保存されます。
ccmH323Device	ccmH323DeviceTable には、Unified Communications Manager (または、クラスタ設定の場合は、ローカルの Unified Communications Manager) に情報が含まれる H.323 デバイスのリストが含まれます。H.323 電話機または H.323 ゲートウェイの場合、ccmH.323DeviceTable には H.323 デバイスごとに 1 つのエントリが作成されます。(H.323 電話機およびゲートウェイは、Unified Communications Manager で登録されません。指定された H.323 電話機およびゲートウェイのコールを処理する準備ができると、Unified Communications Manager によって H.323Started アラームが生成されます。) システムにより、H.323 トランク情報の一部としてゲートキーパー情報が提供されません。

テーブル	コンテンツ
ccmVoiceMailDevice、 ccmVoiceMailDirNum	Cisco uOne、ActiveVoice の場合、ccmVoiceMailDeviceTable には音声メッセージングデバイスごとに1つのエントリが作成されます。登録ステータスに基づいて、Cisc MIB 内の ccmRegisteredVoiceMailDevices、ccmUnregisteredVoiceMailDevices、ccmRejectedVoiceMailDevices カウンタが更新されます。
ccmGateway	ccmRegisteredGateways、ccmUnregisteredGateways、および ccmRejectedGateways は、それぞれ、登録されたゲートウェイ デバイスまたはポートの数、登録されていないゲートウェイ デバイスまたはポートの数、および拒否されたゲートウェイ デバイスまたはポートの数を追跡します。 Unified Communications Manager は、デバイスまたはポート レベルでアラームを生成します。ccmGatewayTable には、CallManager アラームに基づいて、デバイスレベルまたはポートレベルの情報が格納されます。登録済み、未登録、または拒否されたデバイスまたはポートごとに、1つのエントリが ccmGatewayTable に存在します。2つの FXS ポートと1つの T1 ポートを備えた VG200 の場合、ccmGatewayTable には3つのエントリが作成されます。 ccmActiveGateway および ccmInActiveGateway のカウンタは、アクティブな（登録済みの）ゲートウェイ デバイスまたはポート、および接続されていない（未登録または拒否）ゲートウェイ デバイスまたはポートの数を追跡します。 登録ステータスに基づき、ccmRegisteredGateways、ccmUnregisteredGateways、ccmRejectedGateways の各カウンタが更新されます。
ccmMediaDeviceInfo	このテーブルには、少なくとも1回はローカルの Unified Communications Manager での登録を試みたすべてのメディアデバイスのリストが格納されます。
ccmGroup	このテーブルには、Unified Communications Manager クラスタ内の Unified Communications Manager グループが格納されます。
ccmGroupMapping	このテーブルは、クラスタ内のすべての Unified Communications Manager を Unified Communications Manager グループにマッピングします。ローカルの Unified Communications Manager ノードがダウンしても、このテーブルは空のままです。

表 23: CISCO-CCM-MIB の静的テーブル

テーブル	コンテンツ
ccmProductType	このテーブルには、Unified Communications Manager (Unified Communications Manager クラスタ設定の場合はクラスタ) でサポートされる製品タイプのリストが格納されます。タイプには、電話機タイプ、ゲートウェイタイプ、メディア デバイス タイプ、H.323 デバイス タイプ、CTI デバイス タイプ、音声メッセージング デバイス タイプ、SIP デバイス タイプなどがあります。
ccmRegion、ccmRegionPair	ccmRegionTable には、Cisco Communications Network (CCN) システムの地理的に離れた場所にあるすべてのリージョンのリストが格納されます。ccmRegionPairTable には、Unified Communications Manager クラスタの地理的リージョンペアのリストが含まれます。地理的リージョンペアは、接続元リージョンと接続先リージョンで定義されます。
ccmTimeZone	このテーブルには、Unified Communications Manager のクラスタ内のすべてのタイムゾーングループのリストが含まれます。
ccmDevicePool	このテーブルには、Unified Communications Manager のクラスタ内のすべてのデバイスプールのリストが含まれます。デバイスプールは、リージョン、日付/時刻グループ、および Unified Communications Manager グループによって定義されます。



- (注) CISCO-CCM-MIB の「ccmAlarmConfigInfo」グループおよび「ccmQualityReportAlarmConfigInfo」グループでは、通知に関する設定パラメータを定義します。

CISCO-UNITY-MIB

CISCO-UNITY-MIB では、Cisco Unity Connection に関する情報を入手するために Connection SNMP エージェントを使用します。

CISCO-UNITY-MIB の定義を確認するには、次のリンクにアクセスして [SNMP v2 MIB (SNMP v2 MIBs)] をクリックしてください。

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml> [英語]



- (注) Cisco Unity Connection ではこの MIB をサポートしています。Unified Communications Manager と IM and Presence Service は、この MIB をサポートしていません。

Connection SNMP エージェントでは次のオブジェクトをサポートしています。

表 24: CISCO-UNITY-MIB のオブジェクト

オブジェクト	説明
ciscoUnityTable	このテーブルには、ホスト名やバージョン番号など、Cisco Unity Connection サーバに関する一般的な情報が格納されます。
ciscoUnityPortTable	このテーブルには、Cisco Unity Connection のボイスメッセージングポートに関する一般的な情報が格納されます。
General Unity Usage Info オブジェクト	このグループには、Cisco Unity Connection のボイスメッセージングポートの容量と使用率に関する情報が格納されます。

SNMP の設定要件

システムにはデフォルトの SNMP 設定はありません。MIB 情報にアクセスするには、インストール後に SNMP の設定を行う必要があります。シスコでは、SNMP V1、V2c、および V3 バージョンをサポートしています。

SNMP エージェントは、コミュニティ名と認証トラップによるセキュリティを提供します。MIB 情報にアクセスするには、コミュニティ名を設定する必要があります。次の表に、必要な SNMP 構成時の設定を提供します。

表 25: SNMP の設定要件

設定	[Cisco Unified Serviceability] ページ
V1/V2c コミュニティ スtring	SNMP > V1/V2c > コミュニティ スtring
V3 コミュニティ スtring	SNMP > V3 > ユーザ
MIB2 のシステム コンタクトおよびロケーション	SNMP > SystemGroup > MIB2 システム グループ
トラップ通知先 (V1/V2c)	SNMP > V1/V2c > Notification Destination
トラップ通知先 (V3)	SNMP > V3 > Notification Destination

SNMPバージョン1のサポート

SNMPバージョン1 (SNMPv1) は、管理情報構造 (SMI) の仕様の範囲内で機能する SNMP の初期実装で、User Datagram Protocol (UDP) や Internet Protocol (IP) などのプロトコル上で動作します。

SNMPv1 SMI では、高度な構造を持つテーブル (MIB) が定義されます。このテーブルは、表形式のオブジェクト (つまり、複数の変数を含むオブジェクト) のインスタンスのグループ化に使用されます。テーブルにはインデックスが付けられた 0 個以上の行が格納されるため、SNMP では、サポートされているコマンドを使用して、行全体を取得したり変更したりできません。

SNMPv1 では、NMS が要求を発行し、管理対象デバイスから応答が返されます。エージェントは、トラップオペレーションを使用して、NMS に重要なイベントを非同期的に通知します。

有用性 GUI では、[**V1/V2c Configuration**] ウィンドウで SNMPv1 サポートを設定します。

SNMPバージョン2cのサポート

SNMPv2c は、SNMPv1 と同様に、Structure of Management Information (SMI) の仕様の範囲内で機能します。MIB モジュールには、相互に関係のある管理対象オブジェクトの定義が格納されます。SNMPv1 で使用されるオペレーションと SNMPv2 で使用されるオペレーションは、ほぼ同じです。たとえば、SNMPv2 トラップオペレーションは、SNMPv1 で使用する機能と同じですが、異なるメッセージ形式を使用する、SNMPv1 トラップに代わる機能です。

SNMPv2c のインフォーム オペレーションでは、ある NMS から別の NMS にトラップ情報を送信して、その NMS から応答を受信することができます。

有用性 GUI では、[**V1/V2c Configuration**] ウィンドウで SNMPv2c サポートを設定します。

SNMPバージョン3のサポート

SNMPバージョン3は、認証 (要求が正規の送信元から送信されたものかどうかの確認)、プライバシー (データの暗号化)、承認 (要求された操作がユーザに許可されているかどうかの確認)、およびアクセス制御 (要求されたオブジェクトにユーザがアクセスできるかどうかの確認) などのセキュリティ機能を提供します。SNMP パケットがネットワーク上で公開されないようにするには、SNMPv3 を使用して暗号化を設定できます。



- (注) リリース12.5 (1) SU1以降、MD5 または DES 暗号化方式は Unified Communications Manager でサポートされていません。SNMPv3 ユーザの追加時に、認証プロトコルとして SHA または AES を選択できます。

SNMPv1 や v2 などのコミュニティストリングを使用する代わりに、SNMPv3 は SNMP ユーザを使用します。

有用性 GUI で、[**V3 設定 (V3 Configuration)**] ウィンドウで SNMPv3 サポートを設定します。

SNMP サービス

次の表のサービスでは、SNMP の操作をサポートしています。

(注) SNMP マスター エージェントは、MIB インターフェイスのプライマリ サービスとして機能します。Cisco CallManager SNMP サービスは手動でアクティブ化する必要があります。他のすべての SNMP サービスは、インストール後に実行する必要があります。

表 26: SNMP サービス

MIB	サービス	ウィンドウ
CISCO-CCM-MIB	Cisco CallManager SNMP サービス	[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)]。サーバを選択した後、[パフォーマンスおよびモニタリング (Performance and Monitoring)] カテゴリを選択します。
SNMP エージェント	SNMP Master Agent	[Cisco Unified 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)] サーバを選択した後、[Platform Services] カテゴリを選択します。
CISCO-CDP-MIB	CiscoCDP エージェント	
SYSAPPL-MIB	System Application Agent	
MIB-II	MIB2 Agent	
HOST-RESOURCES-MIB	Host Resources Agent	[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)] サーバを選択した後、[プラットフォーム サービス (Platform Services)] カテゴリを選択します。
CISCO-SYSLOG-MIB	Cisco Syslog Agent	[Cisco Unity Connection Serviceability] > [ツール (Tools)] > [サービス管理 (Service Management)] サーバを選択した後、[Base Services] カテゴリを選択します。
ハードウェア MIB	Native Agent Adaptor	
CISCO-UNITY-MIB	Connection SNMP Agent	



注意 SNMP サービスを停止すると、ネットワーク管理システムが Unified Communications Manager または Cisco Unity Connection ネットワークをモニタしなくなるため、データが失われます。テクニカル サポート チームの指示がない限り、サービスを停止しないでください。

SNMP のコミュニティ スtring とユーザ

SNMP コミュニティ スtring では、セキュリティは確保されませんが、MIB オブジェクトへのアクセスを認証し、組み込みパスワードとして機能します。SNMP コミュニティ スtring は、SNMP v1 および v2c の場合にのみ設定します。

SNMPv3 では、コミュニティ スtring を使用しません。バージョン 3 では、代わりに SNMP ユーザを使用します。SNMP ユーザを使用する目的はコミュニティ スtring と同じですが、ユーザの暗号化や認証を設定できるため、セキュリティが確保されます。

Serviceability GUI では、デフォルトのコミュニティ スtring やユーザは存在しません。

SNMP のトラップ とインフォーム

SNMP エージェントは、重要なシステム イベントを識別するために、トラップ形式またはインフォーム形式で NMS に通知を送信します。トラップ形式の場合は宛先からの確認応答を受信しませんが、インフォーム形式の場合は確認応答を受信します。通知先を設定するには、Serviceability GUI の [SNMP 通知先設定 (Notification Destination Configuration)] ウィンドウを使用します。



(注) Unified Communications Manager は、Unified Communications Manager および IM and Presence Service システムの SNMP トラップをサポートします。

SNMP 通知では、対応するトラップ フラグが有効な場合、トラップが即座に送信されます。Syslog エージェントの場合、アラームとシステム レベルのログ メッセージが Syslog デーモンに送信され、ログに記録されます。また、一部の標準的なサードパーティ製アプリケーションでもログ メッセージが syslog デーモンに送信され、ログに記録されます。これらのログ メッセージはローカルの syslog ファイルに記録され、SNMP トラップまたは通知への変換も行われます。

以下に、設定済みのトラップ通知先に送信される、Unified Communications Manager の SNMP のトラップおよびインフォーム メッセージの一覧を示します。

- Unified Communications Manager で障害が発生しました
- Phone failed (電話機で障害が発生)
- Phones status update (電話機ステータスの更新)
- Gateway failed (ゲートウェイで障害が発生)
- Media resource list exhausted (メディア リソース リストが使い果たされた)
- ルート リストの枯渇
- Gateway layer 2 change (ゲートウェイ レイヤ 2 の変更)
- Quality report (品質レポート)
- Malicious call (悪質なコール)

- Syslog message generated (syslog メッセージの生成)



ヒント 通知先を設定する前に、必要な SNMP サービスがアクティブ化され、動作していることを確認します。また、コミュニティ スtring/ユーザに対する特権が正しく設定されていることを確認します。

Serviceability GUI の [SNMP] > [V1/V2] > [通知先 (Notification Destination)] または [SNMP] > [V3] > [通知先 (Notification Destination)] を選択して SNMP トラップの宛先を設定します。

次の表では、ネットワーク管理システム (NMS) で設定するトラップとインフォームのパラメータについて説明します。この表の値を設定するには、その NMS をサポートする SNMP 製品のドキュメントの説明に従って、NMS 上で適切なコマンドを実行します。



(注) 表に記載されているすべてのパラメータは、最後の2つのパラメータを除き、CISCOCCMMIB に含まれています。最後の2つの clogNotificationsEnabled と clogMaxSeverity は、CISCO-SYSLOG-MIB の一部です。

IM and Presence サービスの場合は、NMS で clogNotificationsEnabled および clogMaxSeverity trap/inform パラメータのみを設定します。

表 27: Cisco Unified Communications Manager のトラップおよびインフォーム設定パラメータ

パラメータ名	デフォルト値	生成されるトラップ	推奨設定
ccmCallManagerAlarmEnable	True	ccmCallManagerFailed ccmMediaResourceListExhausted ccmRouteListExhausted ccmTLSConnectionFailure	デフォルトの仕様のままにします。
ccmGatewayAlarmEnable	True	ccmGatewayFailed ccmGatewayLayer2Change Cisco Unified Communications Manager 管理では、CiscoATA 186 デバイスを電話機として設定することができますが、Unified Communications Manager が SNMP トラップを CiscoATA デバイスに送信する際には、ゲートウェイタイプのトラップが送信されます (たとえば、ccmGatewayFailed など)。	なし。デフォルトではこのトラップは有効に設定されています。

パラメータ名	デフォルト値	生成されるトラップ	推奨設定
ccmPhoneStatusUpdateStorePeriod ccmPhoneStatusUpdateAlarmInterval	1800 0	ccmPhoneStatusUpdate	CcmPhoneStatusUpdateAlarmInterval を 30～3600 の値に設定します。
ccmPhoneFailedStorePeriod ccmPhoneFailedAlarmInterval	1800 0	ccmPhoneFailed	ccmPhoneFailedAlarmInterval は 30～3600 の範囲の値に設定します。
ccmMaliciousCallAlarmEnable	True	ccmMaliciousCall	なし。デフォルトではこのトラップは有効に設定されています。
ccmQualityReportAlarmEnable	True	このトラップは、CiscoExtended Functions サービスがサーバ上、または、クラスタ設定の場合には (Unified Communications Manager のみ) ローカル Unified Communications Manager サーバ上でアクティブ化されて実行されている場合にのみ生成されます。 ccmQualityReport	なし。デフォルトではこのトラップは有効に設定されています。
clogNotificationsEnabled	False	clogMessageGenerated	トラップ生成をイネーブルにするには、clogNotificationsEnable を True に設定します。
clogMaxSeverity	警告	clogMessageGenerated	clogMaxSeverity を warning に設定すると、アプリケーションが、シビラティ (重大度) が警告以上の Syslog メッセージを生成したときに SNMP トラップが生成されます。

SFTP サーバのサポート

内部テストでは、Cisco が提供し、Cisco TAC がサポートする Cisco Prime Collaboration Deployment (PCD) 上で SFTP サーバを使用します。SFTP サーバオプションの概要については、次の表を参照してください。

表 28: SFTP サーバのサポート

SFTP サーバ	サポートの説明
Cisco Prime Collaboration Deployment の SFTP サーバ	<p>このサーバはシスコが提供およびテストした SFTP サーバのみであり、Cisco TAC がサポートします。</p> <p>バージョンの互換性は、使用している Emergency Responder および Cisco Prime Collaboration Deployment のバージョンに依存します。バージョン (SFTP) または Emergency Responder をアップグレードする前に、『Cisco Prime Collaboration Deployment Administration Guide』を参照して、互換性のあるバージョンであることを確認してください。</p>
テクノロジー パートナーの SFTP サーバ	<p>これらのサーバはサードパーティが提供およびテストしたものです。バージョンの互換性は、サードパーティによるテストに依存します。テクノロジー パートナーの SFTP サーバまたは Unified Communications Manager をアップグレードする場合、テクノロジー パートナーのページで、互換性のあるバージョンを確認してください。</p> <p>https://marketplace.cisco.com</p>
他のサードパーティの SFTP サーバ	<p>これらのサーバはサードパーティが提供するものであり、Cisco TAC はこれらのサーバを正式にサポートしていません。</p> <p>バージョンの互換性は、SFTP バージョンと Emergency Responder バージョンの互換性を確立するためのベスト エフォートに基づきます。</p> <p>(注) これらの製品がシスコでテストされていない場合、シスコはその機能を保証することができません。Cisco TAC は、これらの製品をサポートしていません。完全にテストされてサポートされる SFTP ソリューションとしては、Cisco Prime Collaboration Deployment またはテクノロジー パートナーの SFTP サーバを利用してください。</p>

SNMP 設定タスク フロー

簡易ネットワーク管理プロトコルの設定を行うには、以下のタスクを実行します。タスクが異なる場合があるため、どの SNMP バージョンを設定するかを必ず確認してください。SNMP V1、V2c、または V3 から選択することができます。

始める前に

SNMP ネットワーク管理システムをインストールして、設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	SNMP サービスの有効化 (201 ページ)	重要な SNMP サービスが稼働中であることを確認します。
ステップ 2	使用する SNMP のバージョンに応じて、以下のいずれかのタスクを実行します。 <ul style="list-style-type: none"> • SNMP コミュニティ スtring の設定 (202 ページ) • SNMP ユーザの設定 (205 ページ) 	SNMP V1 あるいは V2 の場合、SNMP コミュニティ スtring を設定します。 SNMP V3 の場合は、SNMP ユーザを設定します。
ステップ 3	リモート SNMP エンジン ID の取得 (209 ページ)	SNMP V3 の場合は、通知先の設定で必要なリモート SNMP エンジンのアドレスを取得します。 (注) この手順は SNMP V3 では必須ですが、SNMP V1 または V2c ではオプションです。
ステップ 4	SNMP 通知先の設定 (209 ページ)	すべての SNMP バージョンで、SNMP トラップおよび SNMP インフォームの通知先を設定します。
ステップ 5	MIB2 システム グループの設定 (214 ページ)	MIB-II システム グループのシステム コンタクトおよびシステム ロケーションを設定します。
ステップ 6	CISCO-SYSLOG-MIB トラップ パラメータ (216 ページ)	CISCO-SYSLOG-MIB のトラップ設定を設定します。
ステップ 7	CISCO-CCM-MIB トラップ パラメータ (217 ページ)	Unified Communications Manager のみ：CISCO-CCM-MIB のトラップ設定を行います。
ステップ 8	SNMP Master Agent の再起動 (217 ページ)	SNMP の設定が完了したら、SNMP マスター エージェントを再起動します。
ステップ 9	SNMP ネットワーク管理システムで、Unified Communications Manager のトラップ パラメータを設定します。	

SNMP サービスの有効化

SNMP サービスが動作していることを確認するには、以下の手順を使用します。

手順

-
- ステップ 1** [Cisco Unified Serviceability] にログインします。
- ステップ 2** **Cisco SNMP Master Agent** ネットワーク サービスが実行中であることを確認します。サービスはデフォルトでオンになっています。
- [Tools (ツール)] > [Control Center - Network Services (コントロール センタのネットワーク サービス)] を選択します。
 - パブリッシャ ノードを選択し、[移動 (Go)] をクリックします。
 - Cisco SNMP Master Agent** サービスが稼働していることを確認します。
- ステップ 3** **Cisco Call Manager SNMP Service** を起動します。
- [コントロール センター (Control Center)] > [サービスの有効化 (Control Center)] を選択します。
 - [サーバ (Server)] ドロップダウンから、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。
 - Cisco Call Manager SNMP サービス** が稼働していることを確認します。稼働していない場合は、対応するチェック ボックスをオンにして、[保存 (Save)] をクリックします。
-

次のタスク

SNMP V1 または V2c を設定する場合は、[SNMP コミュニティストリングの設定 \(202 ページ\)](#)。

SNMP V3 を設定する場合は、[SNMP ユーザの設定 \(205 ページ\)](#)。

SNMP コミュニティストリングの設定

SNMP V1 または V2c を導入している場合は、以下の手順を使用して SNMP コミュニティストリングを設定します。



-
- (注) この手順は、SNMP V1 または V2c の場合、必須となります。SNMP V3 では、コミュニティストリングではなく SNMP ユーザを設定します。
-

手順

-
- ステップ 1** Cisco Unified Serviceability から、**SNMP > V1/V2c > コミュニティストリング** を選択します。
- ステップ 2** **サーバ** を選択し、**検索** をクリックして、既存のコミュニティストリングを検索します。必要に応じて、検索パラメータを入力して特定のコミュニティ文字列を検索することができます。
- ステップ 3** 次のいずれかを実行します。

- 既存の SNMP コミュニティ ストリングを編集するには、そのストリングを選択します。
- 新しいコミュニティ ストリングを追加するには、[新規追加 (Add New)] をクリックします。

(注) 既存のコミュニティ ストリングを削除するには、そのストリングを選択して、**選択したものを削除する** をクリックします。ユーザを削除したら、Cisco SNMP マスター エージェントを再起動します。

ステップ 4 コミュニティ ストリング名を入力します。

ステップ 5 **SNMP コミュニティ ストリングの設定** ウィンドウの各フィールドに入力します。フィールド およびフィールドの設定の詳細は、[コミュニティ ストリングの構成時の設定 \(203 ページ\)](#) を参照してください。

ステップ 6 **アクセス権限** ドロップダウンで、そのコミュニティ ストリングの権限を設定します。

ステップ 7 この設定をすべてのクラスタ ノードに適用する場合、[すべてのノードに適用 (Apply to All Nodes)] チェック ボックスをオンにします。

ステップ 8 [保存 (Save)] をクリックします。

ステップ 9 **OK** をクリックして、SNMP マスター エージェントのサービスを再起動して、変更を反映させます。

次のタスク

[SNMP 通知先の設定 \(209 ページ\)](#)

コミュニティ ストリングの構成時の設定

次の表で、コミュニティ ストリングの構成時の設定について説明します。

表 29: コミュニティ ストリングの構成時の設定

フィールド	説明
[サーバ (Server)]	<p>コミュニティ ストリングを検索する際に手順を実行してサーバの選択を指定しているため、[コミュニティ ストリング設定 (Community String configuration)] ウィンドウの設定は読み取り専用として表示されます。</p> <p>コミュニティ ストリングのサーバを変更するには、コミュニティ ストリングの検索手順を実行します。</p>

フィールド	説明
コミュニティストリング (Community String)	<p>コミュニティストリングの名前を入力します。この名前には、最長 32 文字を指定でき、英数字、ハイフン (-)、および下線文字 (_) を任意に組み合わせることが可能です。</p> <p>ヒント 部外者が推測しにくいコミュニティストリング名を選択してください。</p> <p>コミュニティストリングを編集するとき、コミュニティストリングの名前は変更できません。</p>
任意のホストからの SNMP パケットを受け入れる (Accept SNMP Packets from any host)	<p>任意のホストから SNMP パケットを受け入れるには、このボタンをクリックします。</p>
指定したホストからの SNMP パケットのみ受け入れる (Accept SNMP Packets only from these hosts)	<p>特定のホストからの SNMP パケットを受け入れるには、このオプションボタンをクリックします。</p> <p>[ホスト名/IPv4/IPv6 アドレス (Hostname/IPv4/IPv6 Address)] フィールドに、SNMP パケットを受け取る IPv4 または IPv6 アドレスを入力し、[挿入 (Insert)] をクリックします。</p> <p>IPv4 アドレスはドット付き 10 進表記です。たとえば、10.66.34.23 と指定します。IPv6 アドレスはコロンで区切られた 16 進表記です。たとえば、2001:0db8:85a3:0000:0000:8a2e:0370:7334 または 2001:0db8:85a3::8a2e:0370:7334 と指定します。</p> <p>SNMP パケットを受け取るアドレスごとにこのプロセスを繰り返します。アドレスを削除するには、それを [ホスト IPv4/IPv6 アドレス (Host IPv4/IPv6 Addresses)] リストボックスから選択し、[削除 (Remove)] をクリックします。</p>

フィールド	説明
アクセス権限 (Access Privileges)	<p>ドロップダウン リスト ボックスで、適切なアクセス レベルを次のリストの中から選択します。</p> <p>ReadOnly</p> <p>コミュニティストリングは、MIB オブジェクトの値の読み取りのみが可能です。</p> <p>ReadWrite</p> <p>コミュニティストリングは、MIB オブジェクトの値を読み書きできます。</p> <p>ReadWriteNotify</p> <p>コミュニティストリングは、MIB オブジェクト値の読み取りおよび書き込みと、トラップおよびインフォームメッセージでの MIB オブジェクト値の送信が可能です。</p> <p>NotifyOnly</p> <p>コミュニティストリングは、トラップおよびインフォームメッセージでの MIB オブジェクト値の送信のみ可能です。</p> <p>ReadNotifyOnly</p> <p>コミュニティストリングは、MIB オブジェクト値の読み取りと、トラップおよびインフォームメッセージでの値の送信が可能です。</p> <p>なし (None)</p> <p>コミュニティストリングはトラップ情報の読み取り、書き込み、送信を行えません。</p> <p>ヒント トラップ設定パラメータを変更するには、NotifyOnly、ReadNotifyOnly、または ReadWriteNotify 権限でコミュニティストリングを設定します。</p> <p>IM and Presence Service は ReadNotifyOnly をサポートしていません。</p>
すべてのノードに適用 (Apply to All Nodes)	<p>クラスタ内のすべてのノードにコミュニティストリングを適用する場合は、このチェックボックスをオンにします。</p> <p>このフィールドは、Unified Communications Manager および IM and Presence Service のクラスタにのみ適用されます。</p>

SNMP ユーザの設定

SNMP V3 を導入している場合は、以下の手順を使用して SNMP ユーザを設定します。



(注) この手順は、SNMP V3 の場合にのみ必要です。SNMP V1 または V2c の場合は、コミュニティストリングを設定します。

手順

ステップ 1 Cisco Unified Serviceability で、**SNMP > V3 > ユーザ**を選択します。

ステップ 2 サーバを選択して、**検索**をクリックして、既存の SNMP ユーザを検索します。必要に応じて、検索パラメータを入力して特定のユーザを検索することができます。

ステップ 3 次のいずれかを実行します。

- 既存の SNMP ユーザを編集するには、ユーザを選択します。
- 新しい SNMP ユーザを追加するには、**新規追加**をクリックします。

(注) 既存のユーザを削除するには、ユーザを選択して**選択したものを削除する**をクリックします。ユーザを削除したら、Cisco SNMP マスター エージェントを再起動します。

ステップ 4 [SNMP User Name] を入力します。

ステップ 5 SNMP ユーザの設定を入力します。フィールドおよびフィールドの設定の詳細は、[SNMP V3 のユーザ構成時の設定 \(207 ページ\)](#) を参照してください。

ヒント 設定を保存する前であれば、[すべてクリア (Clear All)] ボタンをクリックしてウィンドウ内の設定に入力した情報をすべて消去することができます。

ステップ 6 **アクセス権限** ドロップダウンで、このユーザに割り当てるアクセス権限を設定します。

ステップ 7 この設定をすべてのクラスタ ノードに適用する場合、[すべてのノードに適用 (Apply to All Nodes)] チェック ボックスをオンにします。

ステップ 8 [保存 (Save)] をクリックします。

ステップ 9 **OK** をクリックして、SNMP マスター エージェントを再起動します。

(注) 設定したユーザが存在するこのサーバにアクセスするには必ず NMS で適切な認証およびプライバシー設定を使用して、このユーザを設定します。

次のタスク

[リモート SNMP エンジン ID の取得 \(209 ページ\)](#)

SNMP V3 のユーザ構成時の設定

次の表に、SNMP V3 のユーザ構成時の設定について説明します。

表 30: SNMP V3 のユーザ構成時の設定

フィールド	説明
[サーバ (Server)]	<p>通知先の検索の手順を実行したときにサーバを指定済みのため、この設定は読み取り専用として表示されます。</p> <p>アクセスを提供するサーバを変更するには、SNMP ユーザの検索手順を実行します。</p>
ユーザ名 (User Name)	<p>このフィールドには、アクセスを提供するユーザの名前を入力します。この名前には、最長32文字を指定でき、英数字、ハイフン (-)、および下線文字 (_) を任意に組み合わせることが可能です。</p> <p>ヒント ネットワーク管理システム (NMS) に設定済みのユーザを入力します。</p> <p>既存の SNMP ユーザの場合、この設定は読み取り専用として表示されます。</p>
認証を要求 (Authentication Required)	<p>認証を義務付けるには、このチェックボックスをオンにして、[パスワード (Password)] フィールドと [パスワードを再入力 (Reenter Password)] フィールドにパスワードを入力し、適切なプロトコルを選択します。パスワードには 8 文字以上が必要です。</p> <p>(注) FIPS モードまたは拡張セキュリティ モードが有効になっている場合は、プロトコルとして [SHA] を選択します。</p>
プライバシーを要求 (Privacy Required)	<p>[認証を要求 (Authentication Required)] チェックボックスをオンにした場合は、プライバシー情報を指定できます。プライバシーを義務付けるには、このチェックボックスをオンにして、[パスワード (Password)] フィールドと [パスワードを再入力 (Reenter Password)] フィールドにパスワードを入力し、プロトコルのチェックボックスをオンにします。パスワードには 8 文字以上が必要です。</p> <p>(注) FIPS モードまたは拡張セキュリティ モードが有効になっている場合は、プロトコルとして [AES128] を選択します。</p>
任意のホストからの SNMP パケットを受け入れる (Accept SNMP Packets from any host)	<p>任意のホストからの SNMP パケットを受け入れるには、このオプション ボタンをクリックします。</p>

フィールド	説明
指定したホストからの SNMP パケットのみ受け入れる (Accept SNMP Packets only from these hosts)	<p>特定のホストからの SNMP パケットを受け入れるには、このオプションボタンをクリックします。</p> <p>[ホスト名/IPv4/IPv6 アドレス (Hostname/IPv4/IPv6 Address)] フィールドに、SNMP パケットを受け取る IPv4 または IPv6 アドレスを入力し、[挿入 (Insert)] をクリックします。</p> <p>IPv4 アドレスはドット付き 10 進表記です。たとえば、10.66.34.23 と指定します。IPv6 アドレスはコロンで区切られた 16 進表記です。たとえば、2001:0db8:85a3:0000:0000:8a2e:0370:7334 または 2001:0db8:85a3::8a2e:0370:7334 と指定します。</p> <p>SNMP パケットを受け取るアドレスごとにこのプロセスを繰り返します。アドレスを削除するには、それを [ホスト IPv4/IPv6 アドレス (Host IPv4/IPv6 Addresses)] リストボックスから選択し、[削除 (Remove)] をクリックします。</p>
アクセス権限 (Access Privileges)	<p>ドロップダウン リストボックスから、アクセス レベルとして次のいずれかのオプションを選択します。</p> <p>ReadOnly</p> <p>MIB オブジェクトの値の読み取りのみが可能です。</p> <p>ReadWrite</p> <p>MIB オブジェクトの値の読み取りおよび書き込みが可能です。</p> <p>ReadWriteNotify</p> <p>MIB オブジェクトの値の読み取りおよび書き込みと、トラップおよびインフォーム メッセージの MIB オブジェクト値の送信が可能です。</p> <p>NotifyOnly</p> <p>トラップおよびインフォーム メッセージの MIB オブジェクト値の送信のみ可能です。</p> <p>ReadNotifyOnly</p> <p>MIB オブジェクトの値の読み取りと、トラップおよびインフォーム メッセージの値の送信も可能です。</p> <p>なし (None)</p> <p>トラップ情報の読み取り、書き込み、送信を行えません。</p> <p>ヒント トラップ設定パラメータを変更するには、NotifyOnly、ReadNotifyOnly、または ReadWriteNotify 権限でユーザを設定します。</p>

フィールド	説明
すべてのノードに適用 (Apply to All Nodes)	クラスタ内のすべてのノードにユーザ設定を適用する場合は、このチェックボックスをオンにします。 これは、Unified Communications Manager と IM and Presence Service クラスタにのみ適用されます。

リモート SNMP エンジン ID の取得

SNMP V3 を導入する場合は、次の手順を使用して、通知先の設定に必要なリモート SNMP エンジン ID を取得します。



(注) この手順は SNMP V3 では必須ですが、SNMP V1 または 2C ではオプションです。

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 ユーティリティの `snmp walk 1` CLI コマンドを実行します。
- ステップ 3 設定されたコミュニティストリング (SNMP V1/V2) または設定されたユーザ (SNMP V3 を使用) を入力します。
- ステップ 4 サーバの IP アドレスを入力します。たとえば、`localhost` として `127.0.0.1` と入力します。
- ステップ 5 オブジェクト ID (OID) として `1.3.6.1.6.3.10.2.1.1.0` を入力します。
- ステップ 6 ファイルには、`file` と入力します。
- ステップ 7 `y` と入力します。
システムが出力する 16 進数文字列は、リモート SNMP エンジン ID を表します。
- ステップ 8 SNMP が実行されている各ノードでこの手順を繰り返します。

次のタスク

[SNMP 通知先の設定 \(209 ページ\)](#)

SNMP 通知先の設定

この手順を使用して、SNMP トラップおよび通知を送信する通知先を設定します。この手順は、SNMP V1、V2c、または V3 のいずれかでも使用することができます。

始める前に

SNMP コミュニティ スtring あるいは SNMP ユーザが未設定の場合、以下のいずれかのタスクを実行します。

- SNMP V1/V2 については、以下を参照してください。 [SNMP コミュニティ スtring の設定 \(202 ページ\)](#)
- SNMP V3 については、以下を参照してください。 [SNMP ユーザの設定 \(205 ページ\)](#)

手順

-
- ステップ 1** Cisco Unifeid Serviceability で、以下のいずれかを選択します。
- SNMP V1 または V2 の場合、**SNMP > V1 または V2 > 通知先**を選択します
 - SNMP V3 の場合、**SNMP > V3 > 通知先**を選択します
- ステップ 2** サーバを選択して、**検索**をクリックして、既存の SNMP 通知先を検索します。必要に応じて、検索パラメータを入力して特定の通知先を検索することができます。
- ステップ 3** 次のいずれかを実行します。
- 既存の SNMP 通知先を編集するには、通知先を選択します。
 - 新しい SNMP 通知先を追加するには、[新規追加 (Add New)] をクリックします。
- (注) 既存の SNMP 通知先を削除するには、通知先を選択して、**選択したものを削除する**をクリックします。ユーザを削除した後、**Cisco SNMP マスターエージェント**を再起動します。
- ステップ 4** **ホスト IP アドレス** ドロップダウンで、既存のアドレスを選択するか、**新規追加**をクリックして、新しいホスト IP アドレスを入力します。
- ステップ 5** SNMP V1、V2 のみ。SNMP V1 あるいは V2c を設定する場合、いずれかに応じて、**SNMP パージョン** フィールドで、V1 あるいは V2C オプション ボタンをオンにします。
- ステップ 6** SNMP V1 または V2 の場合は、以下の手順を実行します。
- a) SNMP V2 のみ。**通知タイプ** ドロップダウンで、**通知** あるいは **トラップ** を選択します。
 - b) 設定した **コミュニティ スtring** を選択します。
- ステップ 7** SNMP V3 の場合は、以下の手順を実行します。
- a) **通知タイプ** ドロップダウンで、**通知** あるいは **トラップ** を選択します。
 - b) **リモート SNMP エンジン ID** ドロップダウンで、既存のエンジン ID を選択するか、**新規追加** を選択して、新しい ID を入力します。
 - c) **セキュリティ レベル** ドロップダウンで、適切なセキュリティ レベルを割り当てます。
- ステップ 8** この設定をすべてのクラスタ ノードに適用する場合、[**すべてのノードに適用 (Apply to All Nodes)**] チェック ボックスをオンにします。
- ステップ 9** [挿入 (Insert)] をクリックします。

ステップ 10 **OK** をクリックして、SNMP マスター エージェントを再起動します。

例



(注) [通知先の設定] ウィンドウのフィールドの説明については、以下のトピックのいずれかを参照してください。

- [SNMP V1 および V2c の通知先の設定 \(211 ページ\)](#)
- [SNMP V3 の通知先の設定 \(213 ページ\)](#)

次のタスク

[MIB2 システム グループの設定 \(214 ページ\)](#)

SNMP V1 および V2c の通知先の設定

次の表では、SNMP V1/V2c の通知先の構成時の設定について説明します。

表 31: **SNMP V1/V2c** の通知先の構成時の設定

フィールド	説明
[サーバ (Server)]	通知先を検索するための操作です。すでにサーバを指定済みのため、この設定は読み取り専用として表示されます。 通知先のサーバを変更するには、コミュニティ スtring を検索するための手順を実行します。
ホスト IPv4/IPv6 アドレス (Host IPv4/IPv6 Addresses)	ドロップダウン リスト ボックスから、トラップ宛先のホストの IPv4/IPv6 アドレスを選択するか、[新規追加 (Add New)] をクリックします。[新規追加 (Add New)] をクリックした場合は、トラップ宛先の Ipv4/ipv6 アドレスを [ホスト Ipv4/ipv6 アドレス (Host IPv4/ipv6 address)] フィールドに入力します。 既存の通知先の場合、ホストの IP アドレスの設定は変更できません。
ホスト IPv4/IPv6 アドレス	このフィールドに、SNMP パケットを受け取る IPv4 または IPv6 アドレスを入力します。 IPv4 アドレスはドット付き 10 進表記です。たとえば、10.66.34.23 と指定します。IPv6 アドレスはコロンで区切られた 16 進表記です。たとえば、2001:0db8:85a3:0000:0000:8a2e:0370:7334 または 2001:0db8:85a3::8a2e:0370:7334 と指定します。

フィールド	説明
ポート番号	フィールドに、SNMP パケットを受信する宛先サーバ上の通知を受け取るポート番号を入力します。
V1 または V2c (V1 or V2c)	<p>[SNMPバージョン情報 (SNMP Version Information)] ペインで、適切な SNMP バージョンのオプション ボタン ([V1] または [V2c]) をクリックします。これは使用している SNMP のバージョンによります。</p> <ul style="list-style-type: none"> • [V1] を選択した場合は、コミュニティストリングを設定します。 • [V2c] を選択した場合は、通知タイプを設定してからコミュニティストリングを設定します。
[コミュニティストリング (Community String)]	<p>ドロップダウン リスト ボックスから、このホストで生成される通知メッセージに使用するコミュニティ ストリング名を選択します。</p> <p>最小限の通知権限 (ReadWriteNotify または Notify Only) を持つコミュニティ ストリングのみが表示されます。これらの権限を持つコミュニティ ストリングを設定していない場合、ドロップダウン リスト ボックスに選択肢が表示されません。必要に応じて、[Create New UiCommunity String] をクリックして、コミュニティストリングを作成します。</p> <p>IM and Presence のみ：最小限の通知権限 (ReadWriteNotify、ReadNotifyOnly、または Notify Only) を持つコミュニティ ストリングのみが表示されます。これらの権限を持つコミュニティ ストリングを設定していない場合、ドロップダウン リスト ボックスに選択肢が表示されません。必要に応じて、[Create New Community string] をクリックして、コミュニティストリングを作成します。</p>
通知タイプ	ドロップダウンリストボックスから適切な通知タイプを選択します。
すべてのノードに適用 (Apply to All Nodes)	<p>クラスタ内のすべてのノードに通知先の設定を適用する場合は、このチェックボックスをオンにします。</p> <p>これは、Cisco Unified Communications Manager および IM and Presence Service クラスタにのみ適用されます。</p>

SNMP V3 の通知先の設定

次の表では、SNMP V3 の通知先の構成時の設定について説明します。

表 32: SNMP V3 の通知先の構成時の設定

フィールド	説明
[サーバ (Server)]	SNMP V3 の通知先を検索するための操作ですすでにサーバを指定済みのため、この設定は読み取り専用として表示されます。 通知先のサーバを変更するには、SNMP V3 通知先を検索し、別のサーバを選択するための手順を実行します。
ホスト IPv4/IPv6 アドレス (Host IPv4/IPv6 Addresses)	ドロップダウン リスト ボックスから、トラップ宛先のホストの IPv4/IPv6 アドレスを選択するか、[新規追加 (Add New)]をクリックします。[新規追加 (Add New)] をクリックした場合は、トラップ宛先の Ipv4/ipv6 アドレスを [ホスト Ipv4/ipv6 アドレス (Host IPv4/ipv6 address)] フィールドに入力します。 既存の通知先の場合、ホストの IP アドレスの設定は変更できません。
ホスト IPv4/IPv6 アドレス	このフィールドに、SNMP パケットを受け取る IPv4 または IPv6 アドレスを入力します。 IPv4 アドレスはドット付き 10 進表記です。たとえば、10.66.34.23 と指定します。IPv6 アドレスはコロンで区切られた 16 進表記です。たとえば、2001:0db8:85a3:0000:0000:8a2e:0370:7334 または 2001:0db8:85a3::8a2e:0370:7334 と指定します。
ポート番号	フィールドに、宛先サーバ上の通知を受け取るポート番号を入力します。
通知タイプ	ドロップダウン リスト ボックスから [インフォーム (Inform)] または [トラップ (Trap)] を選択します。 ヒント [インフォーム (Inform)] オプションを選択することを推奨します。通知機能では、受信確認されるまでメッセージが再送されるため、トラップよりも信頼性が高くなります。
リモート SNMP エンジン ID (Remote SNMP Engine Id)	この設定は、[通知の種類 (Notification Type)] ドロップダウン リストボックスから [インフォーム (Inform)] を選択した場合に表示されます。 ドロップダウン リスト ボックスからエンジン ID を選択するか、[新規追加 (Add New)] を選択します。[新規追加 (Add New)] を選択した場合は、[リモート SNMP エンジン ID (Remote SNMP Engine Id)] フィールドに 16 進数値で ID を入力します。

フィールド	説明
セキュリティ レベル (Security Level)	<p>ドロップダウン リスト ボックスからユーザに対する適切なセキュリティ レベルを選択します。</p> <p>noAuthNoPriv</p> <p>認証もプライバシーも設定しません。</p> <p>authNoPriv</p> <p>認証を設定しますが、プライバシーは設定しません。</p> <p>authPriv</p> <p>認証とプライバシーを設定します。</p>
[ユーザ情報 (User Information)] ペイン	<p>ペインから、次のいずれかのタスクを実行し、通信先とユーザの間の関連付けを設定または解除します。</p> <ol style="list-style-type: none"> 1. 新しいユーザを作成するには、[新規ユーザの作成 (Create New User)] をクリックします。 2. 既存のユーザを変更するには、ユーザのオプション ボタンをクリックしてから、[選択したユーザの更新 (Update Selected User)] をクリックします。 3. ユーザを削除するには、ユーザのオプション ボタンをクリックしてから、[選択したユーザの削除 (Delete Selected User)] をクリックします。 <p>表示されるユーザは、通知先に設定したセキュリティ レベルに応じて変化します。</p>
すべてのノードに適用 (Apply to All Nodes)	<p>クラスタ内のすべてのノードに通知先の設定を適用する場合は、このチェックボックスをオンにします。</p> <p>これは、Cisco Unified Communications Manager および IM and Presence Service クラスタにのみ適用されます。</p>

MIB2 システム グループの設定

以下の手順で、MIB-II システム グループのシステム コンタクトおよびシステム ロケーションを設定します。たとえば、システムの連絡先として「管理者、555-121-6633」と入力し、システム ロケーションとして「San Jose, Bldg 23, 2nd floor」と入力することができます。この手順は、SNMP V1、V2、および V3 に対して使用できます。

手順

ステップ 1 Cisco Unified Serviceability で、**SNMP > SystemGroup > MIB2 システム グループ** を選択します。

ステップ 2 サーバ ドロップダウンで、ノードを 1 つ選択して、**移動** をクリックします。

ステップ 3 システムの連絡先 および システム ロケーション フィールドの設定を完了します。

ステップ 4 この設定をすべてのクラスタ ノードに適用する場合、[すべてのノードに適用 (Apply to All Nodes)] チェック ボックスをオンにします。

ステップ 5 [保存 (Save)] をクリックします。

ステップ 6 **OK** をクリックして、SNMP マスター エージェント サービスを再起動します。

例



(注) フィールドの説明のヘルプは、以下を参照してください [MIB2 システム グループの設定 \(215 ページ\)](#)



(注) フィールドをクリアするには、**すべてクリア** をクリックします。**すべてクリア** をクリックした後、**保存** をクリックすると、該当の記録が削除されます。

MIB2 システム グループの設定

次の表で、MIB2 システム グループの構成時の設定について説明します。

表 33: MIB2 システム グループの構成時の設定

フィールド	説明
[サーバ (Server)]	ドロップダウン リスト ボックスからコンタクトを設定するサーバを選択し、[移動 (Go)] をクリックします。
システム管理者 (System Contact)	問題が発生したときに知らせる人を入力します。
システムの場所 (System Location)	システム コンタクトとして識別される人の場所を入力します。
すべてのノードに適用 (Apply to All Nodes)	システム設定をクラスタ内のすべてのノードに適用するには、このチェック ボックスをオンにします。 これは、Unified Communications Manager と IM and Presence Service クラスタにのみ適用されます。

CISCO-SYSLOG-MIB トラップパラメータ

システムの CISCO-SYSLOG-MIB トラップ設定を行う場合は次のガイドラインを使用してください。

- SNMP Set 操作を使用して、clogsNotificationEnabled (1.3.6.1.4.1.9.9.41.1.1.2) を True に設定します。たとえば、次のように Linux コマンドラインから net-snmp set ユーティリティを使用してこの OID を True に設定します。

```
snmpset -c <community string> -v2c <transmitter ipaddress>  
1.3.6.1.4.1.9.9.41.1.1.2.0 i 1
```

SNMP Set 操作にはその他の SNMP 管理アプリケーションを使用することもできます。

- SNMP Set 操作を使用して clogMaxSeverity (1.3.6.1.4.1.9.9.41.1.1.3) 値を設定します。たとえば、次のように Linux コマンドラインから net-snmp set ユーティリティを使用してこの OID 値を設定します。

```
snmpset-c public-v2c <transmitter ipaddress> 1.3.6.1.4.1.9.9.41.1.1.3.0 i  
<value>
```

<value>にはシビラティ（重大度）の数値を入力します。値が大きくなるほど、シビラティ（重大度）は低くなります。値 1（緊急）は最も高いシビラティ（重大度）を表し、値 8（デバッグ）は最も低いシビラティ（重大度）を表します。Syslog Agent では、指定した値よりも大きいメッセージは無視されます。たとえば、すべての Syslog メッセージをトラップする場合は値 8 を使用します。

シビラティ（重大度）の値は次のとおりです。

- 1：緊急
- 2：警報
- 3：重大
- 4：エラー
- 5：警告
- 6：通知
- 7：情報
- 8：デバッグ

SNMP Set 操作にはその他の SNMP 管理アプリケーションを使用することもできます。



- (注) 指定されている Syslog バッファ サイズよりも大きいトラップメッセージデータは、ロギング前に Syslog によって切り捨てられます。Syslog トラップメッセージの長さの制限は 255 バイトです。

CISCO-CCM-MIB トラップパラメータ

- SNMP Set 操作を使用して、`ccmPhoneFailedAlarmInterval` (1.3.6.1.4.1.9.9.156.1.9.2) を 30 ~ 3600 の範囲の値に設定します。たとえば、次のように Linux コマンドラインから `net-snmp set` ユーティリティを使用してこの OID 値を設定します。

```
snmpset -c <community string> -v2c <transmitter ipaddress>  
1.3.6.1.4.1.9.9.156.1.9.2 .0 i <value>
```

SNMP Set 操作にはその他の SNMP 管理アプリケーションを使用することもできます。

- SNMP Set 操作を使用して、`ccmPhoneStatusUpdateAlarmInterval` (1.3.6.1.4.1.9.9.156.1.9.4) を 30 ~ 3600 の範囲の値に設定します。たとえば、次のように Linux コマンドラインから `net-snmp set` ユーティリティを使用してこの OID 値を設定します。

```
snmpset -c <community string> -v2c <transmitter ipaddress>  
1.3.6.1.4.1.9.9.156.1.9.4 .0 i <value>
```

SNMP Set 操作にはその他の SNMP 管理アプリケーションを使用することもできます。

CISCO-UNITY-MIB トラップパラメータ

Cisco Unity Connection のみ : Cisco Unity Connection SNMP エージェントはトラップ通知を有効化しませんが、トラップは Cisco Unity Connection アラームによってトリガーできます。Cisco Unity Connection のアラーム定義は、Cisco Unity Connection Serviceability の [アラーム (Alarm)] > [定義 (Definitions)] 画面で確認できます。

CISCO-SYSLOG-MIB を使用してトラップパラメータを設定できます。

関連トピック

[CISCO-SYSLOG-MIB トラップパラメータ](#) (216 ページ)

SNMP Master Agent の再起動

すべての SNMP 設定を完了したら、SNMP Master Agent サービスを再起動します。

手順

- ステップ1 Cisco Unified Serviceability から、[ツール (Tools)] > [コントロールセンター-ネットワークサービス (Control Center - Network Services)] の順に選択します。
- ステップ2 サーバを選択して、**移動**をクリックします。
- ステップ3 **SNMP Master Agent** を選択します。
- ステップ4 [再起動 (Restart)] をクリックします。

SNMP トラップ設定 (SNMP Trap Settings)

CLI コマンドを使用して、設定可能な SNMP トラップの設定を行います。SNMP トラップの設定パラメータと推奨される設定のヒントは、『CISCO SYSLOG-MIB, CISCO-CCM-mib, and CISCO UNITY MIB』に記載されています。

SNMP トラップの設定

SNMP トラップを設定するには、以下の手順を実行します。

始める前に

SNMP 用のシステム設定詳細については、[SNMP 設定タスクフロー \(200 ページ\)](#) を参照してください。

SNMP コミュニティストリング (SNMP V1 または V2 の場合) あるいは SNMP ユーザ (SNMP V3 の場合) の **アクセス権限** が以下のいずれかに設定されていることを確認します。

ReadWriteNotify、**ReadNotify**、**NotifyOnly**。

手順

- ステップ1 CLI にログインし、`utils snmp test` CLI コマンドを実行して、SNMP が実行されていることを確認します。
- ステップ2 [SNMP トラップの生成 \(219 ページ\)](#) に従って、SNMP トラップを生成します (たとえば、`ccmPhoneFailed` または `MediaResourceListExhausted` トラップなど)。
- ステップ3 トラップが生成されない場合は、次の手順を実行します。
 - Cisco Unified Serviceability で、[アラーム (Alarm)] > [設定 (Configuration)] を選択し、[CM サービス (CM Services)] および [Cisco CallManager] を選択します。
 - [すべてのノードに適用 (Apply to All Nodes)] チェックボックスをオンにします。
 - [ローカル Syslog (Local Syslogs)] で、[アラーム イベント レベル (Alarm Event Level)] ドロップダウンリストボックスを [情報 (Informational)] に設定します。

ステップ 4 トラップを再現し、対応するアラームが CiscoSyslog ファイルに記録されるかどうかを確認します。

SNMP トラップの生成

ここでは、特定のタイプの SNMP トラップを生成するプロセスについて説明します。個々のトラップが生成されるようにするには、SNMP をサーバ上でセットアップして実行する必要があります。SNMP トラップを生成するためのシステムのセットアップ方法については、[SNMP トラップの設定 \(218 ページ\)](#) の指示に従ってください。



(注) 個々の SNMP トラップの処理時間は、生成しようとしているトラップによって異なります。SNMP トラップの中には、生成に数分かかる場合があります。

表 34: SNMP トラップの生成

SNMP トラップ	プロセス
ccmPhoneStatusUpdate	<p>ccmPhoneStatusUpdate トラップをトリガーするには：</p> <ol style="list-style-type: none"> 1. ccmAlarmConfig Info mib テーブルで、 ccmPhoneStatusUpdateAlarmInterv (1.3.6.1.4.1.9.9.156.1.9.4) = 30 以上に設定します。 2. Cisco Unified Communications Manager Administration にログインします。 3. Unified Communications Manager に登録され、稼働中の電話機の場合は、電話機をリセットします。 登録解除、次に再登録、Ccmphone Statusupdate トラップを生成します。
ccmPhoneFailed	<p>Ccmphone の失敗したトラップをトリガーするには、次のようにします。</p> <ol style="list-style-type: none"> 1. ccmAlarmConfigInfo mib テーブルで、ccmPhoneFailedAlarmInterval (1.3.6.1.4.1.9.9.156.1.9.2) = 30 以上に設定します。 2. Cisco Unified Communications Manager Administration で、電話の MAC アドレスを無効な値に変更します。 3. Cisco Unified Communications Manager Administration で、電話機の再登録を行います。 4. TFTP サーバ A を指すように電話を設定し、別のサーバに電話を差し込みます。

SNMP トラップ	プロセス
ccmGatewayFailed	<p>CcmGatewayFailed SNMP トラップをトリガーするには、次のようにします。</p> <ol style="list-style-type: none"> 1. CcmGatewayAlarmEnable (1.3.6.1.4.1.9.9.156.1.9.6) が true に設定されていることを確認します。 2. Cisco Unified Communications Manager Administration で、ゲートウェイの MAC アドレスを無効な値に変更します。 3. ゲートウェイをリブートします。
ccmGatewayLayer2Change	<p>レイヤ2がモニタされている動作ゲートウェイで ccmGatewayLayer2Change トラップをトリガーするには、次のようにします (たとえば、のバックホールの負荷)。</p> <ol style="list-style-type: none"> 1. CcmAlarmConfig Info mib テーブルで、ccmGatewayAlarmEnable (1.3.6.1.4.1.9.9.156.1.9.6.0) = true を設定します。 2. Cisco Unified Communications Manager Administration で、ゲートウェイの MAC アドレスを無効な値に変更します。 3. ゲートウェイをリセットします。
MediaResourceListExhausted	<p>MediaResourceListExhausted トラップをトリガーするには：</p> <ol style="list-style-type: none"> 1. Cisco Unified Communications Manager Administration で、標準会議ブリッジリソース (CFB-2) のいずれかを含むメディアリソースグループを作成します。 2. 作成したメディアリソースグループを含むメディアリソースグループリストを作成します。 3. [電話の設定] ウィンドウで、作成したメディアリソースグループリストを、メディアリソースグループリストに設定します。 4. IP Voice Media Streaming サービスを停止します。このアクションにより、ConferenceBridge リソース (CFB-2) が動作を停止します。 5. メディアリソースグループリストを使用する電話で電話会議を発信します。電話画面に「会議ブリッジが使用できません」というメッセージが表示されます。

SNMP トラップ	プロセス
RouteListExhausted	<p>RouteListExhausted トラップをトリガーするには：</p> <ol style="list-style-type: none"> 1. ゲートウェイを1つ含むルート グループを作成します。 2. 作成したルート グループを含むルート グループ リストを作成します。 3. ルートグループリストを使用してコールをルーティングする一意のルートパターンを作成します。 4. ゲートウェイの登録を解除します。 5. いずれかの電話機からのルートパターンと一致する番号をダイヤルします。
MaliciousCallFailed	<p>MaliciousCallFailed トラップをトリガーするには：</p> <ol style="list-style-type: none"> 1. 使用可能なすべての「Maliciouscall」ソフトキーを含むソフトキーテンプレートを作成します。 2. 新しいソフトキーテンプレートをネットワークの電話に割り当てて、電話をリセットします。 3. 電話間で電話をかけます。 4. 通話中に [「Maliciouscall」] ソフトキーを選択します。
ccmCallManagerFailed	<ol style="list-style-type: none"> 1. CallManager アプリケーション ccm のプロセス Id (PID) を取得するには、<code>show process list CLI</code> コマンドを実行します。 このコマンドは、多数のプロセスとそのPidを返します。アラームを生成するために停止する必要がある PID であるため、ccm の PID を取得する必要があります。 2. <code>delete process <pid> crash</code> の CLI コマンドを実行します 3. CLI コマンドを実行します。 <p>CallManager 障害アラームは、内部エラーが発生すると生成されます。これらの内部エラーには、CPU が不足しているために終了した内部スレッド、16秒を超える CallManager サーバの一時停止、およびタイマーの問題が含まれる場合があります。このアラームを手動で生成することはできません。</p> <p>(注) ccmCallManagerFailed アラームまたはトラップを生成して CallManager サービスをシャットダウンし、コアファイルを生成します。混乱を避けるために、コアファイルをただちに削除することを推奨します。</p>

SNMP トラップ	プロセス
トラップとしての syslog メッセージ	<p>特定のシビラティ（重大度）を超える syslog メッセージをトラップとして受信するには、<code>clogBasic</code> テーブルで次の2つの MIB オブジェクトを設定します。</p> <ol style="list-style-type: none"> 1. <code>ClogNotificationsEnabled</code> (1.3.6.1.4.1.9.9.41.1.1.2) を <code>true</code> (1) に設定します。デフォルト値は <code>false</code> (2) です。例：<code>snmpset -c <Community String> -v 2c <transmitter ip address> 1.3.6.1.4.1.9.9.41.1.1.2.0 i 1</code> 2. <code>ClogMaxSeverity</code> (1.3.6.1.4.1.9.9.41.1.1.3) を、トラップを生成するレベルよりも大きいレベルに設定します。デフォルト値は警告 (5) です。 <p>設定されたシビラティ（重大度）レベル以下のアラームシビラティ（重大度）を持つすべての syslog メッセージがトラップとして送信されます。例：<code>snmpset -c <Community String> -v 2c <transmitter ip address> 1.3.6.1.4.1.9.9.41.1.1.3.0 i <value></code></p>

SNMP トレースの設定

Unified Communications Manager の場合、Cisco CallManager SNMP エージェントのトレースを設定するには、Cisco Unified Serviceability の [トレース設定] ウィンドウで、[パフォーマンスおよびモニタリング サービス] サービス グループの [Cisco CallManager SNMP サービス] を選択します。デフォルトの設定は、すべてのエージェントに対して存在します。Cisco CDP Agent および Cisco Syslog Agent の場合、『Cisco Unified Solutions コマンドライン インターフェイス リファレンス ガイド』に従って、CLI を使用してトレース設定を変更します。

Cisco Unity Connection の場合、Cisco Unity Connection SNMP エージェントのトレースを設定するには、Cisco Unity Connection Serviceability の [トレース設定 (Trace Configuration)] ウィンドウで Connection SNMP エージェントのコンポーネントを選択します。

SNMP のトラブルシューティング

トラブルシューティングのヒントについては、この項を参照してください。すべての機能サービスとネットワーク サービスが動作していることを確認してください。

問題

システムから MIB をポーリングできない

この状態は、コミュニティ スtring または SNMP ユーザがシステム上に設定されていないか、システム上に設定されているものと一致しないことを意味します。デフォルトでは、コミュニティ スtring またはユーザはシステムに設定されていません。

解決方法

SNMP の設定ウィンドウを使用して、コミュニティ スtring または SNMP ユーザがシステム上に適切に設定されているかどうかを確認します。

問題

システムから通知を受信できない。

この状態は、通知の宛先がシステム上に正しく設定されていないことを意味します。

解決方法

[通知先 (Notification Destination)] (V1/V2c または V3) 設定ウィンドウで、通知の宛先を正しく設定したことを確認します。



第 16 章

サービス

- [機能サービス \(225 ページ\)](#)
- [ネットワーク サービス \(238 ページ\)](#)
- [サービスのセットアップ \(250 ページ\)](#)

機能サービス

有用性 GUI を使用して、Cisco Unified Communications Manager および IM and Presence サービスをアクティブ化、開始、および停止します。アクティブ化すると、サービスが有効になり、開始されます。使用するすべての機能に対して、機能サービスを手動でアクティブにする必要があります。サービスの有効化に関する推奨事項については、サービスのアクティベーションに関連するトピックを参照してください。



(注) IM and Presence ノードから Unified Communications Manager サーバにアクセスしようとした場合、またはその逆を行おうとした場合、以下のエラーが発生することがあります：「サーバへの接続が確立できません (リモート ノードにアクセスできません)」。このエラーメッセージが表示された場合は、『*Administration Guide for Cisco Unified Communications Manager*』を参照してください。



(注) IM and Presence を使用するデバイスは、永続的なチャット、コンプライアンス、およびファイル転送をサポートするために Postgres 外部データベースを使用するように設定されています。ただし、IM and Presence サーバと Postgres の間の接続は保護されておらず、データはチェックなしで通過します。TLS をサポートしていないサービスまたはデバイスの場合は、通信セッションの各 IP パケットを認証および暗号化することによってセキュアな通信のための標準プロトコルである IP Sec を設定することによって、セキュアな通信を提供するもう1つの方法があります。

[サービスの開始 (Service Activation)] ウィンドウでサービスをアクティブ化した後、[コントロールセンター - 機能サービス (Control Center - Feature Services)] ウィンドウでサービスを起

動する必要はありません。サービスが何らかの理由で起動しなければ、[コントロールセンター - 機能サービス (Control Center - Feature Services)] ウィンドウで起動する必要があります。

システムがインストールされた後は、機能サービスが自動的にアクティブ化されません。機能サービスをアクティブにして、たとえば、有用性レポートアーカイブ機能などの設定機能を使用する必要があります。

Unified Communications Manager および Cisco Unified IM and Presence Service のみ：Unified Communications Manager をアップグレードする場合、アップグレード前にシステムで有効化されているこれらのサービスは、アップグレード後に自動的に起動します。

機能サービスをアクティブにした後、製品の管理 GUI を使用してサービスパラメータの設定を変更できます。

- Cisco Unified Communications Manager Administration
- Cisco Unity Connection の管理

機能サービスのカテゴリ

シスコの統合型の有用性では、[**Service Activation**] ウィンドウと [**Control Center-feature services**] ウィンドウで、機能サービスを次のグループに分類します。

- データベースおよび管理サービス
- パフォーマンスおよびモニタリング サービス
- CM サービス
- CTI サービス
- CDR サービス
- セキュリティ サービス
- ディレクトリ サービス
- Voice Quality Reporter サービス

Cisco Unified IM and Presence の有用性では、[**Service Activation**] ウィンドウと [**Control Center-feature services**] ウィンドウで、機能サービスを次のグループに分類します。

- データベースおよび管理サービス
- パフォーマンスおよびモニタリング サービス
- IM and Presence Service サービス

データベースおよび管理サービス

Locations Bandwidth Manager

このサービスは、IM and Presence サービスではサポートされていません。

Locations Bandwidth Manager サービスは、1 つ以上のクラスタで設定されているロケーションとリンクデータからネットワークモデルを組み立て、2つのロケーション間の有効なパスを決定し、コールのタイプごとの帯域幅の可用性に基づいて2つのロケーション間のコールを許可するかどうかを決定し、許可された各コールの実行期間の帯域幅を差し引きます（予約します）。

Cisco AXL Web Service

Cisco AXL Web Service を使用すると、データベース エントリを変更し、AXL を使用するクライアント ベースのアプリケーションからストアドプロシージャを実行することができます。

IM and Presence Service システムでは、このサービスは Unified Communications Manager と Cisco Unity Connection の両方をサポートします。

Cisco UXL Web サービス

このサービスは、IM and Presence サービスではサポートされていません。

Cisco IP Phone Address Book Synchronizer の TabSync クライアントは、Unified Communications Manager データベースに対するクエリーに Cisco UXL Web サービスを使用します。これにより、Cisco IP Phone Address Book Synchronizer ユーザは自身に関連するエンドユーザデータのみにアクセスすることになります。Cisco UXL Web サービスは、次の機能を実行します。

- エンドユーザが Cisco IP Phone Address Book Synchronizer にログインするときにエンドユーザ名とパスワードを確認することにより、認証チェックを行います。
- 連絡先の一覧表示、取得、更新、削除、追加などの機能を実行するために、現在 Cisco IP Phone Address Book Synchronizer にログインしているユーザだけを承認することにより、ユーザ承認チェックを行います。

Cisco Bulk Provisioning サービス

このサービスは、Cisco Unity Connection をサポートしていません。

設定でクラスタをサポートしている場合（Unified Communications Manager のみ）、Cisco Bulk Provisioning Service は1 台目のサーバでのみ有効化することができます。Unified Communications Manager Bulk Administration Tool を使用して電話とユーザを管理する場合は、このサービスを有効にする必要があります。

Cisco TAPS サービス

このサービスは、Cisco Unity Connection または IM and Presence Service をサポートしていません。

Auto-Registered Phones Support (TAPS) サービス用の Cisco ツールは Cisco Unified Communications Manager Auto-Register Phone Tool をサポートしているため、音声自動応答装置 (IVR) プロンプトにユーザが応答した後、カスタマイズされた設定を自動登録済みの電話にアップロードできます。

クラスタをサポートする設定にした場合 (Unified Communications Manager のみ)、最初のサーバでこのサービスを有効にします。ツール用にダミーの MAC アドレスを作成する場合、Cisco Bulk Provisioning サービスが同じサーバ上でアクティブ化されていることを確認します。



ヒント Cisco Unified Communications Manager Auto-Register Phone Tool は Cisco Customer Response Solutions (CRS) に依存します。ツールが設計どおりに動作できるようにするには、CRS マニュアルで説明されているように CRS サーバを設定し、実行していることを確認します。

Platform Administrative Web サービス

Platform Administrative Web サービスとは、Unified Communications Manager、IM and Presence Service、Cisco Unity Connection システムでアクティブ化され PAWS-M サーバがシステムをアップグレードできるようにすることが可能な Simple Object Access Protocol (SOAP) API です。



重要 PAWS-M サーバで Platform Administrative Web サービスをアクティブ化しないでください。

パフォーマンスおよびモニタリング サービス

Cisco Serviceability Reporter

Cisco Serviceability Reporter サービスは、日次レポートを生成します。詳細については、「有用性レポートのアーカイブ」に関連するトピックを参照してください。

クラスタをサポートする設定の場合 (Unified Communications Manager のみ)、このサービスはクラスタ内のすべての Unified Communications Manager サーバにインストールされます。Reporter は、ログに記録された情報に基づいてレポートを 1 日 1 回生成します。[ツール (Tools)] メニューから、Reporter がシスコのユニファイドサービスで生成するレポートにアクセスできます。各要約レポートは、特定のレポートの統計を示すさまざまなチャートで構成されます。サービスをアクティブ化した後、レポートの生成に最大 24 時間かかる場合があります。

関連トピック

[サービスアビリティ レポートのアーカイブ](#) (331 ページ)

Cisco CallManager SNMP サービス

このサービスは、IM and Presence Service および Cisco Unity Connection をサポートしていません。

このサービスは、CISCO-CCM-MIB を実装し、Unified Communications Manager が使用できるプロビジョニングおよび統計情報に対する SNMP アクセスを提供します。

クラスタをサポートする設定にした場合 (Unified Communications Manager のみ)、クラスタ内のすべてのサーバでこのサービスを有効にします。

CM サービス (CM Services)

ここでは、CM サービスについて説明します。IM and Presence Service および Cisco Unity Connection には適用されません。

Cisco CallManager

Cisco CallManager Service は、ソフトウェアのみのコール処理、また、Unified Communications Manager のシグナリングおよびコール制御機能を提供します。



ヒント Unified Communications Manager クラスタのみ：このサービスを有効化する前に、Cisco Unified Communications Manager 管理で、[Cisco Unified Communications Manager 検索および一覧表示] ウィンドウに Unified Communications Manager サーバが表示されていることを確認してください。サーバが表示されていない場合、このサービスをアクティブ化する前に Unified Communications Manager サーバを追加します。サーバを検索して追加する方法については、『Administration Guide for Cisco Unified Communications Manager』を参照してください。

Unified Communications Manager クラスタのみ：[Service Activation] で Cisco CallManager または CTIManager サービスを無効にした場合、サービスを無効にした Unified Communications Manager サーバはデータベースに存在しなくなります。これは、グラフィカルユーザインターフェイス (GUI) に表示されないため、[Cisco Unified Communications Manager の管理] で設定操作で、該当する Unified Communications Manager サーバを選択できないことを意味します。その後、同じ Unified Communications Manager サーバのサービスを再度有効にすると、データベースに Unified Communications Manager のエントリが再作成され、サーバ名または IP アドレスに「CM_」プレフィックスが追加されます。たとえば、IP アドレスが 172.19.140.180 のサーバで Cisco CallManager または CTIManager サービスを再度有効化した場合は、Cisco Unified Communications Manager Administration に CM_172.19.140.180 と表示されます。これで、新しく「CM_」プレフィックスが追加されたサーバを Administration で選択できるようになりました。

次のサービスには、Cisco CallManager サービスのアクティブ化が必要です。

- [CM サービス \(CM Services\)](#)
- [CDR サービス](#)

Cisco TFTP

Cisco Trivial File Transfer Protocol (TFTP) は、トリビアルファイル転送プロトコル (FTP の簡易バージョン) と整合性のあるファイルを構築し、提供します。Cisco TFTP は、埋め込みコン

ポーネント実行ファイル、リンガー ファイル、デバイス コンフィギュレーション ファイルを提供します。

Unified Communications Manager のみ：設定ファイルには、デバイス（電話およびゲートウェイ）が接続する Unified Communications Manager のリストが含まれます。デバイスをブートすると、コンポーネントは、Dynamic Host Configuration Protocol (DHCP) サーバにそのネットワーク設定情報を照会します。DHCP サーバは応答として、そのデバイスの IP アドレス、サブネットマスク、デフォルトゲートウェイ、ドメインネームシステム (DNS) サーバのアドレス、および TFTP サーバの名前またはアドレスを返します。デバイスは TFTP サーバからコンフィギュレーションファイルを要求します。設定ファイルには、Unified Communications Manager およびデバイスが Unified Communications Manager に接続する際に使用する TCP ポートのリストが含まれます。設定ファイルには、Unified Communications Manager およびデバイスが Unified Communications Manager に接続する際に使用する TCP ポートのリストが含まれます。

Cisco Unified Mobile Voice Access Service

Cisco Unified Voice Access Service は、Cisco Unified Mobility 内のモバイル ボイス アクセス機能を起動します。モバイルボイスアクセスは自動音声応答 (IVR) システムで、この機能により Cisco Unified Mobility ユーザは次のタスクを実行できます。

- コールがデスクフォンから発信されたかのように携帯電話から発信します。
- Cisco Unified Mobility を有効にします。
- Cisco Unified Mobility を無効にします。

Cisco IP Voice Media Streaming App

Cisco IP Voice Media Streaming Application サービスは、メディア ターミネーション ポイント (MTP)、会議、保留音 (MoH)、およびアナウンサーに使用する音声メディア ストリーミング機能を Unified Communications Manager に提供します。Cisco IP Voice Media Streaming Application は、Unified Communications Manager から、リアルタイム プロトコル (RTP) ストリーミングを処理する IP 音声メディア ストリーミング ドライバにメッセージをリレーします。

Cisco IP Voice Media Streaming Application サービスは、会議、MOH、アナウンサー、MTP などの IP Voice Media Streaming Application コンポーネントを含むコール レッグの呼管理レコード (CMR) ファイルは生成しません。

Cisco CTI Manager

Cisco CTI Manager には、アプリケーションと対話する CTI コンポーネントが含まれます。このサービスにより、アプリケーションは電話機と仮想デバイスをモニタまたは制御して、コール制御機能を実行できます。

Unified Communications Manager クラスタのみ：CTI Manager を使用すると、アプリケーションはクラスタのすべての Unified Communications Manager のリソースおよび機能にアクセスすることができ、フェールオーバー機能が向上します。1つのクラスタでは1つまたは複数の CTI Manager をアクティブにできますが、個々のサーバに置くことのできる CTI Manager は1つだ

けです。1つのアプリケーション（JTAPI/TAPI）を複数の CTI Manager に同時に接続できますが、1つのアプリケーションがメディアターミネーションを持つデバイスを開くために使用できる接続は、一度に1つだけです。

Cisco エクステンション モビリティ

このサービスは、Cisco Extension Mobility機能をサポートしており、この機能のログインおよび自動ログアウト機能を実行します。

Cisco Dialed Number Analyzer

Dialed Number Analyzer サービスは、Unified Communications Manager Dialed Number Analyzer をサポートしています。アクティブ化すると、このアプリケーションによって大量のリソースが消費されるため、このサービスはコール処理の中断が最小限になるオフピーク時にのみ実行してください。

Cisco Unified Communications Manager クラスタの場合のみ：このサービスをクラスタ内のすべてのサーバで有効化することは推奨されません。このサービスは、コール処理作業が最も少ないクラスタのサーバの1つでのみアクティブにすることを推奨します。

Cisco Dialed Number Analyzer Server

Cisco Dialed Number Analyzer Server サービスは Cisco Dialed Number Analyzer サービスとともに、Cisco Unified Communications Manager Dialed Number Analyzer をサポートします。このサービスは、Cisco Dialed Number Analyzer サービス専用のノードでのみアクティブ化する必要があります。

Cisco Unified Communications Manager クラスタの場合のみ：このサービスをクラスタ内のすべてのサーバで有効化することは推奨されません。このサービスは、コール処理作業が最も少ないクラスタのサーバの1つでのみアクティブにすることを推奨します。

Cisco DHCP Monitor サービス

Cisco DHCP Monitor サービスは、データベース テーブルで、IP Phone の IP アドレスの変更をモニタします。変更が検出されると、`/etc./dhcpd.conf` ファイルを変更し、DHCPD デーモンを再起動します。

シスコ クラスタ間検索サービス

Intercluster Lookup Service (ILS) は、クラスタ全体をベースとして実行されます。ILS を使用すると、リモートの Unified Communications Manager クラスタのネットワークを作成することができます。ILS クラスタ検出機能を使用すると、管理者が各クラスタ間の接続を手動で設定しなくても、Cisco Unified Communications Manager からリモートクラスタに接続できるようになります。ILS グローバルダイヤルプランレプリケーション機能は、ILS ネットワーク内のクラスタがグローバルダイヤルプランデータを ILS ネットワーク内の他のクラスタと交換できるようにします。

ILS の有効化は、Cisco Unified Communications Manager 管理で、**高度な機能 > ILS 設定** を選択して、[ILS 設定]ウィンドウで行うことができます。

Cisco UserSync サービス

Cisco UserSync サービスは、Unified Communications Manager のエンド ユーザ テーブルのデータを LDAP データベースに同期します。

Cisco UserLookup Web Service

Cisco UserLookup Web Service は、商用コール（外部ゲートウェイ経由のコール）を着信側の内線の代替番号に転送して、外線番号に電話する際の商用コストがかからないようにします。

Unified Communications Manager ネットワーク内の発信者が外線番号にコールを発信する場合、Unified Communications Manager は内部番号が LDAP データベースの着信側に存在するかどうかを確認します。内線番号がある場合、そのコールはその内線番号に転送されます。LDAP データベースに内線番号がない場合は、そのコールは元の（外線の）番号に転送されます。

Cisco Headset Service

互換性のある Cisco IP Phone、Cisco Jabber、またはその他のシスコデバイスを使用している場合、Cisco Headset サービスによるシスコヘッドセットのインベントリ、設定の更新、および診断データの管理が可能です。



-
- (注) Cisco ヘッドセットサービスは、Cisco CallManager サービスがすでに実行されているすべての Unified Communications Manager ノードでアクティブにする必要があります。Cisco Unified CM の管理インターフェイスを使用して、ヘッドセットを管理する Unified Communications Manager ノードで Cisco ヘッドセットサービスをアクティブにしてください。Cisco ヘッドセットサービスを有効にすると、Cisco CallManager サービスは自動的にアクティブになります。不要な場合は、Cisco CallManager サービスを非アクティブにします。
-

IM and Presence サービス

IM and Presence サービスは IM and Presence Service だけに適用されます。

Cisco SIP Proxy

Cisco SIP Proxy サービスは、SIP レジストラとプロキシ機能を提供します。これには、要求のルーティング、要求者の識別、および転送の相互接続が含まれます。

Cisco Presence Engine

Cisco Presence Engine は標準ベースの SIP および SIMPLE インターフェイスを使用して、ユーザの機能と属性を収集、集約、および配布します。また、可用性ステータスとユーザの通信機能に関する情報を収集します。

Cisco XCP Text Conference Manager

Cisco XCP Text Conference Manager はチャット機能をサポートします。チャット機能を使用すると、ユーザは、オンラインチャットルームで互いにコミュニケーションできます。アドホック（一時的）なチャットルームと、永続的（削除しない限りシスコがサポートする外部データベースに保持される）なチャットルームを使用したチャット機能がサポートされています。

Cisco XCP Web Connection Manager

Cisco XCP Web Connection Manager サービスでは、ブラウザベースのクライアントを IM and Presence Service に接続できます。

Cisco XCP Connection Manager

Cisco Unified Presence XCP Connection Manager は、XCP クライアントが Cisco Unified Presence サーバに接続できるようにします。

Cisco XCP SIP Federation Connection Manager

Cisco XCP SIP Federation Connection Manager は、Microsoft OCS を使用した SIP プロトコルでのドメイン間フェデレーションをサポートします。展開に IM and Presence Service リリース 9.0 クラスタと Cisco Unified Presence リリース 8.6 クラスタとの間のクラスタ間接続が含まれる場合、このサービスもオンにする必要があります。

Cisco XCP XMPP Federation Connection Manager

Cisco XCP XMPP Federation Connection Manager は XMPP プロトコル経由での IBM Lotus Sametime、Cisco Webex Meeting Center、GoogleTalk などのサードパーティ エンタープライズとのドメイン間フェデレーション、および XMPP プロトコル経由での別の IM and Presence Service エンタープライズとのドメイン間フェデレーションをサポートします。

Cisco XCP Message Archiver

Cisco XCP Message Archiver サービスは、IM コンプライアンス機能をサポートします。IM コンプライアンス機能は、ポイントツーポイントメッセージ、チャット機能のアドホック（一時的）なチャットルームと永続的なチャットルームからのメッセージなど、IM and Presence Service サーバとの間で送受信されたすべてのメッセージを記録します。メッセージは、シスコがサポートする外部データベースに記録されます。

Cisco XCP Directory Service

Cisco XCP Directory Service は、XMPP クライアントと LDAP ディレクトリの統合をサポートします。これにより、ユーザが LDAP ディレクトリの連絡先を検索または追加できるようになります。

Cisco XCP Authentication Service

Cisco XCP Authentication Service は、IM and Presence Service に接続する XMPP クライアントからのすべての認証要求を処理します。

CTI サービス

ここでは、CTI サービスについて説明します。Cisco Unity Connection または IM and Presence Service には適用されません。

Cisco IP マネージャーアシスタント

このサービスは、Cisco Unified Communications Manager Assistant をサポートしています。サービスをアクティブ化すると、Cisco Unified Communications Manager Assistant によってマネージャとアシスタントがより効率的に連携できるようになります。Cisco Unified Communications Manager Assistant は、プロキシ回線サポートと共有回線サポートという 2 種類の動作モードをサポートしています。

この機能は、コールルーティング サービス、マネージャに対する電話機能の機能拡張、そして主にアシスタントによって使用されるデスクトップインターフェイスで構成されています。

このサービスは、マネージャ宛でのコールを代行受信し、これを事前に設定されたコールフィルタに基づいて選択したアシスタント、マネージャ、または他の宛先にルーティングします。マネージャはコールルーティングを動的に変更することができます。たとえば、電話機のソフトキーを押すと、すべてのコールをアシスタントにルーティングするようサービスに指示したり、それらのコールの状態を受信したりすることができます。

Unified Communications Manager のユーザは、マネージャとアシスタントで構成されます。ルーティングサービスは、マネージャのコールをインターセプトし、それらを適切にルーティングします。アシスタントユーザはマネージャに代わってコールを処理します。

Cisco WebDialer Web Service

Cisco Unified Communications Manager システム用の Cisco WebDialer Web サービス

Cisco WebDialer にはクリックツーダイヤル機能があります。この機能を使用すると、Unified Communications Manager のクラスタ内のユーザが、Web ページやデスクトップアプリケーションを使用して、クラスタ内およびクラスタ外の他のユーザに対してコールを発信することができます。Cisco WebDialer には、ユーザがクラスタ内で相互に通話するための Web ページが用意されています。Cisco WebDialer は、WebDialer Servlet と Redirector Servlet という 2 つのコンポーネントで構成されています。

リダイレクターサーブレットは、サードパーティ製アプリケーションが Cisco Web Dialer を使用するための機能を提供します。Redirector Servlet は Cisco Web Dialer ユーザのための適切な Unified Communications Manager のクラスタを検出し、そのクラスタの Cisco Web Dialer に要求をリダイレクトします。Redirector 機能は Simple Object Access Protocol (SOAP) ベースの Web Dialer アプリケーションでは使用できないため、HTTP または HTML ベースの Web Dialer クライアントアプリケーションでのみ使用できます。

セルフプロビジョニング IVR

セルフプロビジョニング IVR サービスの導入により、Unified Communications Manager に自動登録された IP フォンをより少ない作業量で、より早くユーザに割り当てることができます。

IVR サービスを使用するユーザの内線番号から、[セルフプロビジョニング (Self-Provisioning)] ページで設定された CTI RP DN にダイヤルすると、電話がセルフプロビジョニング IVR アプリケーションに繋がり、セルフサービス クレデンシャルの提供が求められます。入力したセルフサービス クレデンシャルが正しければ、IVR サービスによって自動登録された IP フォンがユーザに割り当てられます。

サービスがアクティブになっていない場合でもセルフプロビジョニングを設定できますが、管理者は IVR サービスを使用して IP 電話をユーザに割り当てることはできません。このサービスはデフォルトでは非アクティブ化されています。

セルフプロビジョニング IVR サービスを有効にするには、Cisco CTI Manager サービスも有効にする必要があります。

セルフプロビジョニング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。

CDR サービス

ここでは、CDR サービスについて説明します。IM and Presence Service および Cisco Unity Connection には適用されません。

CAR Web サービス

Cisco CAR Web サービスは CAR のユーザインターフェイスをロードします。CAR は CDR データを使用して CSV 形式または PDF 形式のレポートを生成する Web ベースのレポート アプリケーションです。

Cisco SOAP - CDRonDemand Service

SOAP または HTTPS ベースのサービスである Cisco SOAP - CDRonDemand サービスは、CDR Repository サーバで実行されます。ユーザが指定した間隔（最大 1 時間）に基づく CDR ファイル名のリストに対する SOAP 要求を受信し、要求で指定された時間内に収まるファイル名のリストを返します。また、このサービスは要求で指定されたファイル名と転送方式（SFTP または FTP、サーバ名、ログイン情報、ディレクトリ）を持つ特定の CDR/CMR ファイルの配信に対する要求も受信します。

HTTPS または SOAP インターフェイスを通じて CDR データにアクセスするサードパーティ製の課金アプリケーションを使用している場合は、このサービスをアクティブにします。

Unified Communications Manager リリース 12.x と以降のリリースの場合、CDR onDemand Service は、デフォルトで有効になっていません。CDR onDemand Service を有効にする場合、このサービスを手動でアクティブにする必要があります。CDR onDemand Service をアクティブにするには、`/usr/local/cm/bin/soapservicecontrol2.shCDRonDemandServiceCDRonDemanddeploy8443` コマンドを実行します。

セキュリティ サービス

この項では、セキュリティ サービスについて説明します。IM and Presence Service および Cisco Unity Connection には適用されません。

Cisco CTL Provider

Unified Communications Manager のみ：ローカル システム アカウント権限で実行される Cisco CTL Provider サービスは、クライアント側のプラグインである Cisco CTL Provider Utility と連携し、クラスタのセキュリティ モードを非セキュア モードから混合モードに変更します。このプラグインをインストールすると、Cisco CTL Provider サービスは、CTL ファイルのクラスタ内のすべての Unified Communications Manager および Cisco TFTP サーバのリストを取得します。ここには、クラスタ内のセキュリティ トークンおよびサーバのリストが含まれます。

Cisco CTL クライアントまたは CLI コマンドセット **ユーティリティ CTL** をインストールして設定し、クラスタ全体のセキュリティモードを非セキュアからセキュアに変更するために、このサービスをアクティブにすることができます。

サービスをアクティブ化すると、Cisco CTL Provider サービスはデフォルト CTL ポート (2444) に戻ります。ポートを変更する場合の詳細については、『*Cisco Unified Communications Manager Security Guide*』を参照してください。

Cisco Certificate Authority Proxy Function (CAPF)

Certificate Authority Proxy Function (CAPF) アプリケーションと連携することで、CAPF サービスは設定に応じて次のタスクを実行できます。

- サポートされている Cisco Unified IP 電話モデルにローカルで有効な証明書を発行します。
- 電話の既存の証明書をアップグレードします。
- トラブルシューティング用に電話の証明書を取得します。
- 電話のローカルで有効な証明書を削除します。



(注) Unified Communications Manager のみ：Real-Time Monitoring Tool (RTMT) でリアルタイム情報を表示する場合、CAPF サービスは最初のサーバにのみ表示されます。

ディレクトリ サービス

ここでは、ディレクトリ サービスについて説明します。IM and Presence Service および Cisco Unity Connection には適用されません。

Cisco DirSync

Unified Communications Manager : Cisco DirSync サービスを使用すると、Unified Communications Manager のデータベースにすべてのユーザ情報が保存されます。たとえば、Microsoft Active

Directory や Netscape/iPlanet Directory などの統合された社内ディレクトリを Unified Communications Manager に使用している場合、Cisco DirSync サービスはユーザーデータを Unified Communications Manager データベースに移行します。Cisco DirSync サービスは社内ディレクトリのパスワードを同期しません。



- (注) 重複する電子メール Id を持つユーザは同期されず、管理者は、同期されていないユーザのリストに関する通知を受信しません。これらの ID は、ユニファイド RTMT の DirSync エラーログに表示されます。

Cisco Unity Connection : Cisco Unity Connection が LDAP ディレクトリと統合されている場合、Cisco DirSync サービスは LDAP ディレクトリ内の対応するデータと Cisco Unity Connection サーバ上の Unified Communications Manager のデータベース内のユーザーデータ（氏名、エイリアス、電話番号など）の小規模なサブセットを同期します。別のサービス（CuCmDbEventListener）では、Unified Communications Manager のデータベースのデータと Cisco Unity Connection ユーザーデータベースのデータを同期します。Cisco Unity Connection クラスタが設定されている場合、Cisco DirSync サービスはパブリッシュ サーバだけで実行されます。

ロケーションベースのトラッキング サービス

ここでは、ロケーションベースのトラッキングサービスについて説明します。

Cisco Wireless Controller Synchronization サービス

このサービスは、ネットワークのワイヤレス アクセス ポイントと関連モバイル デバイスのステータスを提供するロケーション認識機能をサポートします。

このサービスは、Unified Communications Manager とシスコのワイヤレス アクセス ポイントコントローラを同期するためにも実行する必要があります。サービスが動作し、同期が設定されると、Unified Communications Manager は、データベースとシスコのワイヤレス アクセス ポイントコントローラを同期し、コントローラが管理するワイヤレス アクセス ポイントのステータス情報を保存します。最新の情報となるように、一定の間隔で同期が実行されるようにスケジューリング設定できます。



- (注) 新しいシスコワイヤレスアクセスポイントコントローラを追加するときに、このサービスが実行されていることを確認してください。

Voice Quality Reporter Services

この項では、Voice Quality Reporter サービスについて説明します。IM and Presence Service および Cisco Unity Connection には適用されません。

Cisco Extended Functions

Cisco Extended Functions サービスは、Quality Report Tool (QRT) など、Unified Communications Manager の音声品質機能のサポートを提供します。個々の機能の詳細については、『*System Configuration Guide for Cisco Unified Communications Manager*』および『*Cisco Unified IP Phone Administration Guide for Cisco Unified Communications Manager*』を参照してください。

ネットワーク サービス

ネットワーク サービスは自動的にインストールされ、データベースサービスやプラットフォーム サービスなど、システムが動作するために必要なサービスが含まれます。これらのサービスは、基本機能に必要なため [サービスのアクティブ化 (Service Activation)] ウィンドウで有効にできません。トラブルシューティングのためなど、必要に応じて [コントロールセンター - ネットワーク サービス (Control Center - Network Services)] ウィンドウで、ネットワーク サービスを停止してから起動 (または再起動) する必要があります。

アプリケーションのインストール後、ネットワーク サービスは [コントロールセンター - ネットワーク サービス (Control Center - Network Services)] ウィンドウで指定されたとおりに自動的に起動します。有用性 GUI は、サービスを論理グループに分類します。

パフォーマンスおよびモニタリング サービス (Performance and Monitoring Services)

Cisco CallManager のサービスアビリティ RTMT

Cisco CallManager Serviceability RTMT サブレットは、トレースの収集と表示、パフォーマンス モニタリング オブジェクトの表示、アラートの処理、システム パフォーマンスとパフォーマンス カウンタのモニタなどを実行できる IM and Presence Real-Time Monitoring Tool (RTMT) をサポートします。

Cisco RTMT Reporter Servlet

Cisco RTMT Reporter サブレットを使用すると、RTMT にレポートをパブリッシュできます。

Cisco Log Partition Monitoring Tool

Cisco Log Partition Monitoring Tool サービスは、設定済みのしきい値とポーリング間隔を使用して、ノード (またはクラスタ内のすべてのノード) 上のログパーティションのディスク使用率をモニタするログパーティションモニタリング機能をサポートします。

Cisco Tomcat Stats Servlet

Cisco Tomcat Stats Servlet は RTMT または CLI を使用して Tomcat perfmon カウンタをモニタすることができます。このサービスが CPU 時間などのリソースを大量に使用していることが疑われる場合を除き、このサービスを停止しないでください。

Cisco RIS Data Collector

Real-time Information Server (RIS) は、デバイス登録ステータス、パフォーマンス カウンタ統計、生成された重大アラームなどのリアルタイム情報を保持します。Cisco RIS Data Collector サービスは、IM and Presence Real-Time Monitoring Tool (RTMT)、SOAP アプリケーションなどのアプリケーションに、クラスタ内のすべての RIS ノードに格納された情報を取得するためのインターフェイスを提供します。

Cisco AMC Service

リアルタイムモニタリングツール (RTMT) に使用されます。このサービス、アラートマネージャ、およびコレクタサービスにより、RTMT はサーバ(またはクラスタ内のすべてのサーバ)に存在するリアルタイム情報を取得できます。

Cisco Audit Event Service

Cisco Audit Event Service は、ユーザによる、またはユーザ処理の結果による Unified Communications Manager または IM and Presence システムへの管理設定のすべての変更をモニタし、記録します。Cisco Audit Event Service は、ログイン、ログアウト、IM チャットルームの入退場などのエンド ユーザ イベントもモニタし、記録します。

バックアップおよび復元サービス

Cisco DRF Master

これは IM and Presence サービスには適用されません。

CiscoDRF Master Agent サービスは、Disaster Recovery System GUI または CLI と連携して必要に応じてバックアップのスケジューリング、復元の実行、依存関係の表示、ジョブステータスの確認、ジョブの取り消しを行う DRF Master Agent をサポートします。Cisco DRF Master Agent は、バックアップおよび復元プロセス用のストレージメディアも提供します。

Cisco DRF Local

Cisco DRF Local サービスは、DRF Master Agent の主要部分である Cisco DRF Local Agent をサポートします。コンポーネントは、ディザスタ リカバリ フレームワークを使用するために Cisco DRF Local Agent に登録されます。Cisco DRF Local Agent は、Cisco DRF Master Agent から受信したコマンドを実行します。Cisco DRF Local Agent は、ステータス、ログ、およびコマンド結果を Cisco DRF Master Agent に送信します。

System Services

Cisco CallManager のサービスアビリティ

Cisco CallManager Serviceability サービスは、問題をトラブルシューティングし、サービスを管理するために使用する Web アプリケーション/インターフェイスである Cisco Unified Serviceability および IM and Presence Service Serviceability GUI をサポートしています。自動的にインストー

ルされるこのサービスは Serviceability GUI にアクセスできます。サーバでこのサービスを停止すると、そのサーバを参照するときに Serviceability GUI にアクセスできません。

Cisco CDP

Cisco Discovery Protocol (CDP) は音声アプリケーションを他のネットワーク管理アプリケーションにアドバタイズするため、ネットワーク管理アプリケーション (SNMP や Cisco Unified Operations Manager など) が、音声アプリケーション用のネットワーク管理タスクを実行できるようにします。

Cisco Trace Collection Servlet

Cisco Trace Collection Servlet は、Cisco Trace Collection サービスとともにトレース収集をサポートし、ユーザが RTMT を使用してトレースを表示できるようにします。サーバ上でこのサービスを停止すると、そのサーバ上のトレースは収集または表示ができなくなります。

SysLog ビューアと Trace and Log Central が RTMT で動作するためには、Cisco Trace Collection Servlet と Cisco Trace Collection Service がサーバで動作している必要があります。

Cisco Trace Collection Service

Cisco Trace Collection サービスは、Cisco Trace Collection Servlet とともにトレース収集をサポートし、ユーザが RTMT クライアントを使用してトレースを表示できるようにします。サーバ上でこのサービスを停止すると、そのサーバ上のトレースは収集または表示ができなくなります。

SysLog ビューアと Trace and Log Central が RTMT で動作するためには、Cisco Trace Collection Servlet と Cisco Trace Collection Service がサーバで動作している必要があります。



ヒント 必要に応じて初期化時間を短くし、Cisco Trace Collection Servlet を再起動する前に Cisco Trace Collection サービスを再起動することを推奨します。

プラットフォーム サービス

Cisco DB

Cisco DB サービスは、Unified Communications Manager 上での Progres データベース エンジンをサポートしています。IM and Presence Service では、A Cisco DB サービスは IDS データベース エンジンをサポートします。

Cisco DB Replicator

Unified Communications Manager および IM and Presence のみ : Cisco DB Replicator サービスは、データベース設定と、クラスタ内の最初のサーバとその他サーバの間でデータ同期を確認します。

Cisco Tomcat

Cisco Tomcat サービスは Web サーバをサポートします。

SNMP Master Agent

このサービスはエージェントプロトコルエンジンとして機能し、SNMP 要求に関連する認証、許可、アクセス コントロール、およびプライバシーの機能を提供します。



ヒント Serviceability GUI で SNMP の設定を完了した後、[コントロールセンター—ネットワーク機能 (Control Center—Network Features)] ウィンドウで SNMP Master Agent サービスを再起動する必要があります。

MIB2 Agent

このサービスは、システム、インターフェイス、IP など、変数の読み取りおよび書き込みを行う、RFC 1213 で定義されている変数に対する SNMP アクセスを提供します。

Host Resources Agent

このサービスは、ストレージリソース、プロセステーブル、デバイス情報、およびインストールされたソフトウェア ベースなど、ホスト情報に対する SNMP アクセスを提供します。このサービスは HOST-RESOURCES-MIB を実装します。

Native Agent Adaptor

このサービスは、ベンダーの Management Information Bases (MIB) をサポートしており、SNMP 要求を、システム上で実行されている別の SNMP エージェントに転送できます。

IM and Presence Service および Unified Communications Manager では、仮想マシンにインストールされた場合、このサービスは提供されません。

System Application Agent

このサービスは、システム上にインストールされ、実行されているアプリケーションに対する SNMP アクセスを提供します。これは SYSAPPL-MIB を実装します。

Cisco CDP Agent

このサービスは、ノードのネットワーク接続情報に対する SNMP アクセスを提供するために Cisco Discovery Protocol を使用します。このサービスは CISCO-CDP-MIB を実装します。

Cisco Syslog Agent

このサービスでは、さまざまな Unified Communications Manager コンポーネントが生成する syslog メッセージの収集をサポートします。このサービスは CISCO-SYSLOG-MIB を実装します。



注意 SNMP サービスを停止すると、ネットワーク管理システムがネットワークをモニタしなくなるため、データが失われます。テクニカル サポート チームの指示がない限り、サービスを停止しないでください。

Cisco Certificate Change Notification

このサービスによって、Tomcat、CallManager、XMPP などのコンポーネントの証明書がクラスタ内のすべてのノードで自動的に同期されます。サービスが停止し、証明書を再生成した場合には、他のノードの証明書信頼に証明書を手動でアップロードする必要があります。

Platform Administrative Web サービス

Platform Administrative Web サービスとは、Unified Communications Manager、IM and Presence Service、Cisco Unity Connection システムでアクティブ化され PAWS-M サーバがシステムをアップグレードできるようにすることが可能な Simple Object Access Protocol (SOAP) API です。



重要 PAWS-M サーバで Platform Administrative Web サービスをアクティブ化しないでください。

Platform Communication Web Service

Platform Communication Web Service は、Unified Communications Manager、Unified Communications Manager、IM and Presence Service、および Cisco Unity Connection システム上で実行される、Representational State Transfer Protocol (REST) API です。



(注) **Platform Communication Web Service** を手動で起動あるいは停止することはできません。

Cisco UDS Tomcat

このサービスは、他の Web アプリケーションの速度を低下させたり、GUI を遅くしたりアクセスできなくなったりする、UDS での大量のリソース使用を回避します。

Cisco AXL Tomcat

このサービスは、他の Web アプリケーションの速度を低下させたり、GUI を遅くしたりアクセスできなくなったりする、AXL での大量のリソース使用を回避します。

Cisco SSOSP Tomcat

このサービスは、他の Web アプリケーションの速度を低下させたり、GUI を遅くしたりアクセスできなくなったりする、SSOSP での大量のリソース使用を回避します。

Cisco Certificate Expiry Monitor

このサービスは、システムが生成する証明書の有効期限切れのステータスを定期的に確認し、証明書の有効期限に近づくと、通知を送信します。Unified Communications Manager では、Cisco Unified Operating System Administration で、このサービスを使用する証明書を管理します。IM and Presence Serviceでは、Cisco Unified IM and Presence Operating System Administration でこのサービスを使用する証明書を管理します。

Cisco Smart License Manager

Cisco Smart License Manager は、パブリッシャでのみ実行されるネットワークサービスです。Unified Communications Manager パブリッシャ上のすべての Cisco Smart Licensing 処理を管理します。Cisco Smart License Manager サービスは、製品のライセンスまたは権限付与の使用状況を Cisco Smart Software Manager または Cisco Smart software Manager サテライトに報告し、Cisco Smart Software Manager または Cisco Smart Software Manager から認証ステータスを取得します。衛星。

セキュリティ サービス

Cisco Certificate Enrollment Service

このサービスは、オンラインのサードパーティ CA および認証局のプロキシ機能の間にオンライン接続を構築します。LSC 証明書に署名するために認証局のプロキシ機能を備えたオンライン CA を使用するには、このサービスをアクティブにする必要があります。

シスコ信頼検証サービス

このサービスは、IM and Presence Service ではサポートされません。

Cisco Trust 検証サービスは、電話機やその他のエンドポイントに代わって証明書を認証する、CallManager サーバまたは専用サーバ上で実行されているサービスです。証明書の所有者のロールのリストを関連付けます。証明書または所有者を1つまたは複数のロールに関連付けることができます。

電話と信頼検証サービス間のプロトコルにより、電話は検証を要求できます。信頼検証サービスは証明書を検証し、それに関連付けられたロールのリストを返します。プロトコルは、信頼検証サービスが要求を認証できるようにし、逆に電話は信頼検証サービスからの応答を認証できるようにします。プロトコルは、要求と応答の整合性を保護します。要求の機密性と応答は必要ありません。

Cisco Trust 検証サービスの複数のインスタンスは、拡張性を提供するために、クラスタ内の異なるサーバ上で実行されます。これらのサーバは、Cisco Unified CallManager をホストするサーバと同じであっても、同じでなくてもかまいません。電話はネットワーク内の信頼検証サービスのリストを取得し、選択アルゴリズム（ラウンドロビンなど）を使用してそのいずれかに接続します。接続されている信頼検証サービスが応答しない場合、電話機はリスト内の次の信頼検証サービスに切り替えます。

データベース サービス

Cisco Database Layer Monitor

Cisco Database Layer Monitor サービスは、データベース層の局面をモニタします。このサービスは、変更通知とモニタリングを扱います。



- (注) Unified Communications Manager で使用される Automatic Update Statistics は、データベーステーブルに加えられた変更をモニタし、統計の更新を必要とするテーブルのみを更新する、インテリジェントな統計更新機能です。この機能により、とりわけ Unified Communications Manager の VMware 導入で、帯域幅が大幅に節約されます。インデックスは、デフォルトで Automatic Update Statistics によって作成されます。

SOAP サービス

Cisco SOAP-Real-Time Service APIs

IM and Presence Service のみ：Cisco SOAP-Real-Time Service API は、プレゼンス データのためのクライアント ログインおよびサードパーティ API をサポートします。

Unified Communications Manager および Cisco Unity Connection のみ：Cisco SOAP-Real-Time Service API により、デバイスと CTI アプリケーションのリアルタイム情報を収集することができます。このサービスは、サービスのアクティブ化、起動、停止のための API も提供します。

Cisco SOAP-パフォーマンスモニタリング Api

Cisco SOAP-Performance Monitoring API サービスは、さまざまなアプリケーションで SOAP API を通じてパフォーマンス モニタリング カウンタを使用できるようにします。たとえば、サービスごとのメモリ情報、CPU 使用率、パフォーマンス モニタリング カウンタなどをモニタできます。

Cisco SOAP ログ収集 Api

Cisco SOAP-Log Collection API サービスは、ログ ファイルを収集し、リモート SFTP サーバのログ ファイルの収集スケジュールを設定できるようにします。収集するログ ファイルの例としては、syslog、コア ダンプ ファイル、シスコ アプリケーション トレース ファイルなどがあります。

SOAP-Diagnostic Portal Database サービス

Cisco ユニファイドリアルタイムモニタリングツール (RTMT) は、SOAP 診断ポータルデータベースサービスを使用して、RTMT Analysis Manager のホストデータベースにアクセスします。RTMT は、オペレータが定義したフィルタの選択に基づいてコールレコードを収集します。このサービスが停止している場合、RTMT はデータベースからコールレコードを収集できません。

CM サービス (CM Services)

ここでは、Unified Communications Manager CM サービスについて説明します。Cisco Unity Connection および Cisco Unity Connection には適用されません。

Cisco Extension Mobility アプリケーション

Cisco のエクステンション モビリティ アプリケーション サービスでは、Cisco エクステンション モビリティ機能の電話機設定の接続時間制限などのログイン設定を定義することができます。

Unified Communications Manager のみ：Cisco Extension Mobility 機能により、Unified Communications Manager クラスタ内のユーザは、クラスタ内の別の電話機にログインして、その電話機を一時的に自分自身の電話機として設定できます。ユーザがログインすると、電話機にユーザの個人の電話番号、スピードダイヤル、サービスリンク、その他のユーザ固有のプロパティが反映されます。ログアウト後、電話機には元のユーザプロファイルが反映されません。

Cisco User Data Services

Cisco User Data Services により、Cisco Unified IP 電話は Cisco Unified Communications Manager データベースのユーザデータにアクセスできます。シスコのユーザデータサービスは、シスコのパーソナルディレクトリのサポートを提供します。

シスコのプッシュ通知サービス

Cisco プッシュ通知サービスは、着信コールのプッシュ通知を Cisco Unified Communications Manager から Apple iOS デバイスに送信する機能を提供します。このサービスは、Cisco CallManager サービスから Cisco Collaboration Cloud にプッシュ通知メッセージをリレーします。このサービスは、プッシュ通知の送信に使用されるアクセストークンも管理します。

Cisco ヘッドセットサービス

互換性のある Cisco IP Phone、Cisco Jabber、またはその他のシスコ デバイスを使用している場合、Cisco Headset サービスによるシスコヘッドセットのインベントリ、設定の更新、および診断データの管理が可能です。



- (注) Cisco ヘッドセットサービスは、Cisco CallManager サービスがすでに実行されているすべての Unified Communications Manager ノードでアクティブにする必要があります。Cisco Unified CM の管理インターフェイスを使用して、ヘッドセットを管理する Unified Communications Manager ノードで Cisco ヘッドセットサービスをアクティブにしてください。Cisco ヘッドセットサービスを有効にすると、Cisco CallManager サービスは自動的にアクティブになります。不要な場合は、Cisco CallManager サービスを非アクティブにします。

IM and Presence Service サービス

IM and Presence Service サービスは IM and Presence Service だけに適用されます。

Cisco Login Datastore

Cisco Login Datastore は、Cisco Client Profile Agent にクライアント セッションを保存するためのリアルタイム データベースです。

Cisco Route Datastore

Cisco Route Datastore は、Cisco SIP Proxy と Cisco Client Profile Agent のルート情報と割り当て済みユーザのキャッシュを保存するためのリアルタイム データベースです。

Cisco Config Agent

Cisco Configuration Agent は、IM and Presence Service IDS データベースの設定変更を Cisco SIP プロキシに通知する変更通知サービスです。

Cisco Sync Agent

Cisco Sync Agent は、IM and Presence データと Unified Communications Manager データの同期を維持します。IM and Presence に重要なデータについて Unified Communications Manager に SOAP 要求を送信し、Unified Communications Manager からの変更通知にサブスクライブして IM and Presence IDS データベースを更新します。

Cisco OAM Agent

Cisco OAM Agent サービスは、プレゼンス エンジンに関する IM and Presence Service IDS データベースの設定パラメータを監視します。データベースに変更が発生すると、OAM Agent がコンフィギュレーションファイルにその内容を書き込み、プレゼンス エンジンに RPC 通知を送信します。

Cisco Client Profile Agent

Cisco Client Profile Agent サービスは、HTTPS を使用した外部クライアントとの間の安全な SOAP インターフェイスを提供します。

Cisco Intercluster Sync Agent

Cisco Intercluster Sync Agent サービスは、Unified Communications Manager への DND の伝播を可能にし、クラスタ間 SIP ルーティングのために IM and Presence Service クラスタの間でエンドユーザ情報を同期します。

Cisco XCP ルータ

XCP ルータは IM and Presence Service サーバのコア コミュニケーション機能です。IM and Presence Service で XMPP ベースのルーティング機能を提供します。XMPP データを IM and Presence Service 上の他のアクティブな XCP サービスにルーティングしたり、SDNS にアクセスして、システムが XMPP データを IM and Presence Service ユーザにルーティングできるように

にします。XCP ルータはユーザの XMPP セッションを管理し、これらのセッションとの間で XMPP メッセージをルーティングします。

IM and Presence Service のインストール後に、システムは Cisco XCP Router をデフォルトでオンにします。



- (注) Cisco XCP ルータを再起動すると、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。Cisco XCP Router を再起動するには、[再起動 (Restart)] オプションを選択する必要があることに注意してください。これは、Cisco XCP Router を停止して起動するのとは違います。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しません。手動で他の XCP サービスを起動する必要があります。

Cisco XCP Config Manager

Cisco XCP Config Manager サービスは、他の XCP コンポーネント（ルータや Message Archiver など）に影響がある、管理 GUI による設定とシステム トポロジの変更（およびクラスターピアから同期されたトポロジ変更）をモニタし、必要に応じてこれらのコンポーネントを更新します。Cisco XCP Config Manager サービスは、これらの変更により XCP コンポーネントの再起動が必要な場合、管理者向けの通知を作成し、再起動が完了すると自動的に通知をクリアします。

Cisco Server Recovery Manager

Cisco Server Recovery Manager (SRM) サービスは、プレゼンス冗長グループ内のノード間のフェールオーバーを管理します。SRM は、ノード内のすべての状態変化を管理します。状態変化には、自動的なものと管理者により実行されるもの（手動）があります。プレゼンス冗長グループのハイアベイラビリティを有効にすると、各ノードの SRM がピアノードとのハートビート接続を確立し、重要なプロセスのモニタを開始します。

Cisco IM and Presence Data Monitor

Cisco IM and Presence Data Monitor は IM and Presence Service の IDS レプリケーションステータスを監視します。他の IM and Presence サービスは、Cisco IM and Presence Data Monitor に依存します。これらの依存サービスは、シスコサービスを使用して IDS のレプリケーションステータスが安定するまで起動を遅らせます。

また、Cisco IM and Presence Data Monitor は、Unified Communications Manager から Cisco Sync Agent の同期のステータスを確認します。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 Unified Communications Manager からの同期を完了させた後にのみ、依存するサービスを起動することができます。タイムアウトが発生すると、IDS レプリケーションおよび Sync Agent が完了していない場合でも、パブリッシャノードの Cisco IM and Presence Data Monitor により依存するサービスの起動が許可されます。

サブスクリバノードでは、IDS レプリケーションが正常に確立されるまで Cisco IM and Presence Data Monitor は機能サービスの起動を遅らせます。Cisco IM and Presence Data Monitor

は、クラスタ内の問題のあるサブスクライバノードのみで機能サービスの起動を遅らせます。1台のノードで問題があっても、すべてのサブスクライバノードで機能サービスの起動が遅れることはありません。たとえばIDSレプリケーションがnode1およびnode2で正常に確立されていても、node3で確立されていない場合、Cisco IM and Presence Data Monitorは機能サービスをnode1およびnode2で起動しますが、node3では起動を遅らせます。

Cisco Presence Datastore

Cisco Presence Datastoreは、一時的なプレゼンスデータとサブスクリプションを格納するためのリアルタイムデータベースです。

Cisco SIP Registration Datastore

Cisco Presence SIP Registration Datastoreは、SIP登録データを保存するためのリアルタイムデータベースです。

Cisco RCC Device Selection

Cisco RCC Device Selectionサービスはリモートコール制御のためのCisco IM and Presenceユーザのデバイス選択サービスです。

CDR サービス

ここでは、CDRサービスについて説明します。IM and Presence ServiceおよびCisco Unity Connectionには適用されません。

Cisco CDR Repository Manager

このサービスは、Cisco CDR Agentサービスから取得された、生成されたコール詳細レコード（CDR）を維持し、移動します。クラスタがサポートされているシステム（Unified Communications Managerのみ）では、このサービスは最初のサーバにあります。

Cisco CDR Agent



- (注) Unified Communications Managerは、Cisco Unified Communications ManagerシステムのCisco CDR Agentをサポートします。

このサービスは、IM and Presence ServiceおよびCisco Unity Connectionをサポートしていません。

Cisco CDR Agentサービスは、Unified Communications Managerによって生成されるCDRファイルおよびCMRファイルを、ローカルホストからCDRリポジトリサーバに転送します。このサーバでは、CDR Repository ManagerサービスがSFTP接続を使用して実行されます。

このサービスは、ローカルホストから生成されたCDRおよびCMRファイルを、クラスタ内のCDR repositoryサーバに転送します。CDR Repository ノードスタンドアロンサーバのCDR

エージェントは、SFTP 接続を介してスタンドアロンサーバによって生成されたファイルを Cisco CDR Repository Manager に転送します。CDR Agent はファイルを維持して移動します。

このサービスを機能させるには、サーバで Cisco CallManager サービスをアクティブにし、サービスが実行されていることを確認します。設定でクラスタがサポートされている場合 (Unified Communications Manager のみ)、最初のサーバ上で Cisco CallManager サービスをアクティブ化します。

Cisco CAR Scheduler

Cisco CDR Analysis and Reporting (CAR) スケジューラサービスは、IM and Presence サービスと Cisco Unity Connection をサポートしていません。

Cisco CAR Scheduler サービスを使用すると、レポートの生成や、CDR 分析とレポート (CAR) データベースへの CDR ファイルのロードなど、CAR に関連するタスクをスケジュールできます。

Cisco SOAP CallRecord サービス

Cisco SOAP CallRecord サービスは、パブリッシャ上では、soap サーバとしてデフォルトで実行されるため、クライアントは SOAP API を介して CAR データベースに接続できます。この接続は、CAR コネクタを使用して実行されます (別の CAR ID インスタンスがある場合)。

Cisco CAR DB

Cisco CAR DB は、CAR データベースの Informix インスタンスを管理します。これにより、サービスマネージャはこのサービスを開始または停止したり、CAR IDS インスタンスをそれぞれ起動またはシャットダウンしたりできます。これは、CCM IDS インスタンスを維持するために使用される Unified Communications Manager データベースに似ています。

Cisco CAR DB サービスは、デフォルトでパブリッシャでアクティブになります。Car DB インスタンスは、CAR データベースを維持するために、パブリッシャ上でインストールされ、アクティブに実行されます。このネットワークサービスはパブリッシャでのみ使用され、サブスクリバでは使用できません。

インストール

ここでは、管理サービスについて説明します。Cisco Unity Connection には適用されません。

Cisco CallManager Administration

Cisco CallManager Admin サービスは、IM and Presence Service および Cisco Unity Connection ではサポートされていません。

Cisco CallManager Admin サービスは、Unified Communications Manager Administration (Cisco Unified Communications Manager 設定を構成するために使用する Web アプリケーション/インターフェイス) をサポートします。Unified Communications Manager のインストール後に、このサービスは自動的に起動し、グラフィカルユーザインターフェイス (GUI) にアクセスすることができるようになります。このサービスを停止すると、そのサーバをブラウズしたとき

に、Cisco Unified Communications Manager Administration のグラフィカル ユーザ インターフェイスにアクセスできません。

Cisco IM and Presence Admin

Cisco IM and Presence 管理サービスは、Unified Communications Manager および Cisco Unity Connectionではサポートされません。

Cisco IM and Presence Admin サービスは、Cisco Unified Communications Manager IM and Presence 管理、つまりIM and Presence Service 設定を行うために使用する Web アプリケーション/インターフェイス) をサポートします。IM and Presence Serviceをインストールした後、このサービスが自動的に起動し、GUIにアクセスできるようになります。このサービスを停止すると、そのサーバをブラウズする際に、Cisco Unified Communications Manager IM and Presence 管理 GUI にアクセスできなくなります。

サービスのセットアップ

コントロールセンター

Serviceability GUI のコントロールセンターでは、ステータスを表示したり、一度に1つのサービスを起動および停止したりすることができます。ネットワークサービスを起動、停止、および再起動するには、[コントロールセンター-ネットワーク サービス (Control Center - Network Services)] ウィンドウにアクセスします。機能サービスを起動、停止、再起動するには、[コントロールセンター-機能サービス (Control Center - Feature Services)] ウィンドウにアクセスします。



ヒント [関連リンク (Related Links)] リストボックスと[移動 (Go)] ボタンを使用して、[コントロールセンター (Control Center)] ウィンドウと[サービスの開始 (Service Activation)] ウィンドウにナビゲートします。

Unified Communications Manager および IM and Presence のみ：クラスタ設定では、ステータスを表示したり、クラスタ内の1台のサーバのサービスを一度に開始および停止することができます。

Unified Communications Manager のみ：機能サービスを起動および停止すると、そのサービスに現在登録されているすべての Cisco Unified IP Phone およびゲートウェイがセカンダリ サービスにフェールオーバーされます。セカンダリ サービスに登録できない場合だけデバイスと電話機を再起動する必要があります。サービスを起動および停止すると、Unified Communications Manager をホームとするその他のインストール済みアプリケーション (会議ブリッジまたは Cisco Messaging Interface など) も起動および停止します。



注意 Unified Communications Manager のみ：サービスを停止すると、そのサービスによって制御されるすべてのデバイスの呼処理も停止します。サービスが停止すると、IP フォンから別の IP フォンへのコールは停止せず、IP フォンからメディア ゲートウェイ コントロール プロトコル (MGCP) ゲートウェイへの進行中のコールも停止しませんが、他の種類のコールはドロップします。

サービスのセットアップ

サービスを使用する場合は、次のタスクを実行できます。

手順

- ステップ 1** 実行する機能サービスをアクティブ化します。
- ステップ 2** 適切なサービス パラメータを設定します。
- ステップ 3** 必要に応じて、Serviceability GUI のトレースツールを使って問題のトラブルシューティングを行います。

サービス アクティベーション



- (注) Serviceability GUI の [サービスの開始 (Service Activation)] ウィンドウでは、複数の機能サービスをアクティブ化または非アクティブ化したり、アクティブ化するデフォルトのサービスを選択できます。IM and Presence のノードから Unified Communications Manager サービスの表示、起動、停止を行ったり、その逆を行うことができます。次のエラーが発生することがあります。「サーバへの接続が確立できません(リモート ノードにアクセスできません) (Connection to the Server cannot be established (unable to access Remote Node))」。このエラー メッセージが表示された場合は、『*Administration Guide for Cisco Unified Communications Manager*』を参照してください。



- (注) Unified Communications Manager Release 6.1.1 以降、エンドユーザはサービスの起動および停止に Cisco Unified Serviceability を利用することができません。

機能サービスは自動モードでアクティブ化され、Serviceability GUI により、単一ノード構成に基づいてサービスの依存関係がチェックされます。機能サービスをアクティブ化することを選択すると、動作するためにそのサービスに依存するサービスが他にある場合は、そのすべてを選択することが求められます。[デフォルトの設定 (Set Default)] をクリックすると、サーバで実行するために必要なサービスが Serviceability GUI によって選択されます。

Cisco Unified Communications Manager および IM and Presence Service のみ：クラスタをサポートする設定であっても、このプロセスは単一サーバ設定に基づきます。

サービスをアクティブ化すると、自動的にサービスが起動します。サービスはコントロールセンターから開始および停止します。

Cisco Unified Communications Manager のクラスタ サービス アクティベーションに関する推奨事項

クラスタでサービスを有効化する前に、マルチサーバ Unified Communications Manager 設定用のサービスの推奨事項を示す、次の表を確認してください。

表 35: Cisco Unified Communications Manager のサービス アクティベーションに関する推奨事項

サービス/サブレット	アクティブ化の推奨事項
CM サービス	
Cisco CallManager	<p>このサービスは、Unified Communications Manager をサポートしています。</p> <p>[Control Center - Network Services] で、Cisco RIS Data Collector サービスと Database Monitor サービスがノードで実行されていることを確認します。</p> <p>ヒント このサービスをアクティブ化する前に、Cisco Unified Communications Manager Administration 内の [Unified Communications Manager の検索/リスト (Cisco Unified Communications Manager Find/List)] ウィンドウの Unified Communications Manager サーバの表示内容を確認します。サーバが表示されていないこのサービスをアクティブ化する前に Unified Communications Manager サーバを追加します。</p> <p>サーバを追加する方法については、『<i>System Configuration Guide for Unified Communications Manager</i>』を参照してください。</p>
Cisco Messaging Interface	サーバに接続された USB/シリアルアダプタを使用してサードパーティ製ボイスシステムとの SMDI 統合を使用している場合にだけアクティブ化します。
Cisco Unified Mobile Voice Access Service	モバイル ボイス アクセスが機能するには、最初の VXML ページを指すようにゲートウェイを設定した後でクラスタ内の最初のノードでこのサービスをアクティブする必要があります。また、Cisco CallManager および Cisco TFTP サービスはタ内の 1 つのサーバ上で実行するようにしてください。Cisco Unified Mobile Voice Access Service が実行されているサーバと同じサーバである必要はありません。
Cisco IP Voice Media Streaming App	クラスタ内に複数のノードがある場合は、クラスタごとに 1 つまたは 2 つのサーバをアクティブ化します。保留音専用のノードでアクティブ化することができます。サービスでは、クラスタ内の 1 つのノードで Cisco TFTP をアクティブ化する必要があります。最初のノードおよび Cisco CallManager サービスを実行するノードでは、サービスをアクティブ化しないでください。

サービス/サブレット	アクティブ化の推奨事項
Cisco CTIManager	JTAPI/TAPI アプリケーションが接続する各ノードでアクティブ化します。CTIManager をアクティブ化するには、Cisco CallManager サービスもノードでアクティブ化する必要があります。CTIManager および Cisco CallManager サービスの相互作用の詳細については、CM サービスに関連するトピックを参照してください。
Cisco エクステンション モビリティ	クラスタ内のすべてのノードでアクティブ化します。
Cisco Extended Functions	Quality Report Tool (QRT) をサポートするこのサービスは、Cisco RIS Data Collector を実行する 1 つまたは複数のサーバでアクティブ化します。クラスタ内のすべてのノードで CTIManager サービスがアクティブなことを確認します。
Cisco DHCP Monitor サービス	DHCP Monitor Service が有効になると、IP フォンの IP アドレスに影響するネットワークの変更を検出し、/etc/dhcpd.conf ファイルを変更し、DHCPD を停止し、更新コンフィギュレーションファイルで再起動します。このサービスは、DHCPD が実行されているノード上でアクティブ化してください。
シスコ ロケーション帯域幅マネージャ	音声コールとビデオ コールの帯域幅割り当てを管理するために Cisco の Location Bandwidth Manager コールアドミッション制御メカニズムを使用する場合は、このサービスをアクティブ化する必要があります。このサービスは、Cisco CallManager サービスとともに実行されます。Cisco CallManager サービスを実行するサーバで Cisco Location Bandwidth Manager を実行することを推奨します。CallManager サービスと同じサーバで Location Bandwidth Manager が実行されていない場合は、Location Bandwidth Manager グループが定義されていることを確認します。
シスコ クラスタ間検索 サービス	複数の Unified Communications Manager クラスタ間で URI と数字ルーティンクを交換する場合、この交換に参加するクラスタのパブリッシャでこのサービスをアクティブ化する必要があります。
Cisco Dialed Number Analyzer Server	クラスタ内に複数のノードがある場合は、Cisco Dialed Number Analyzer サービスの 1 つのノードでこのサービスをアクティブにしてください。
Cisco Dialed Number Analyzer	Unified Communications Manager の Dialed Number Analyzer を使用する場合は、このサービスをアクティブ化します。このサービスはリソースを大量に消費することため、コール処理アクティビティが最も少ないノードかオフピーク時にアクティブ化します。
Cisco TFTP	クラスタ内に複数のノードがある場合は、Cisco TFTP サービス専用の 1 つのノードでこのサービスをアクティブ化します。クラスタ内の複数のノードでこのサービスをアクティブ化する場合は、オプション 150 を設定します。

サービス/サブレット	アクティブ化の推奨事項
Cisco Headset Service	<p>Unified Communications Manager からシスコヘッドセットを管理する場合は、このサービスを有効化します。</p> <p>(注) Cisco ヘッドセットサービスは、Cisco CallManager サービスがすでにアクティブ化されているすべての Unified Communications Manager ノードでアクティブにする必要があります。Cisco Unified CM の管理インターフェイスを使用して、ヘッドセットを管理する Unified Communications Manager ノードで Cisco ヘッドセットサービスをアクティブにしてください。Cisco ヘッドセットサービスを有効にすると、Cisco CallManager サービスは自動的にアクティブになります。不要な場合は、Cisco CallManager サービスを非アクティブにします。</p>
CTI サービス	
Cisco IP Manager Assistant	<p>Cisco Unified Communications Manager Assistant を使用する場合は、クラスタ内の 2 台のサーバ（プライマリおよびバックアップ）でこのサービスをアクティブにします。Cisco CTI Manager サービスがクラスタ内でアクティブ化されていることを確認します。</p> <p>Cisco IP Manager Assistant の詳細については、『<i>Feature Configuration Guide for Unified Communications Manager</i>』を参照してください。</p>
Cisco WebDialer Web Service	クラスタごとに 1 つのノードでアクティブ化します。
セルフプロビジョニング IVR	<p>セルフプロビジョニング IVR サービスを有効にするには、Cisco CTI Manager サービスも有効にする必要があります。</p> <p>サービスがアクティブになっていない場合でもセルフプロビジョニングを設定しますが、管理者は IVR サービスを使用して IP 電話をユーザに割り当てることはできません。このサービスはデフォルトでは非アクティブ化されています。</p>
CDR サービス	
Cisco SOAP-CDRonDemand サービス	<p>Cisco SOAP-CDRonDemand サービスは、最初のサーバ上だけでアクティブ化することができ、Cisco CDR Repository Manager および Cisco CDR Agent サービスが同じサーバ上で実行されている必要があります。</p> <p>Unified Communications Manager リリース 12.x と以降のリリースの場合、CDR onDemand Service は、デフォルトで有効になっていません。CDR onDemand Service を有効にする場合、このサービスを手動でアクティブにする必要があります。CDR onDemand Service をアクティブにするには、<code>/usr/local/cm/bin/soap-service-control2.sh CDRonDemandService CDRonDemanddep</code> コマンドを実行します。</p>

サービス/サブレット	アクティブ化の推奨事項
Cisco CAR Web Service	Cisco CAR Web サービスは、最初のサーバ上だけでアクティブ化することができ、CAR Scheduler サービスが同じサーバ上でアクティブにされ、実行されており、Repository Manager サービスも同じサーバ上で実行されている必要があります。
データベースおよび管理者サービス	
Cisco AXL Web Service	インストール後は、すべてのクラスタ ノードで Cisco AXL Web サービスが有効になります。パブリッシャ ノードではこのサービスを常にアクティブ化することを推奨します。これにより、Unified Provisioning Manager などの AXL を使用する製品を設定できるようになります。 必要に応じて、機能サービス下の Cisco Unified Serviceability の特定のサブレットのサービスをアクティブ化/非アクティブ化することができます。
Cisco Bulk Provisioning サービス	Cisco Bulk Provisioning サービスは、最初のノードだけでアクティブにできる Administration Tool (BAT) を使用して電話とユーザを管理している場合は、サービスをアクティブ化する必要があります。
Cisco UXL Web サービス	このサービスは、認証およびユーザ許可のチェックを実行します。Cisco IP Phone Address Book Synchronizer の TabSync クライアントは、Cisco Unified Communications Manager データベースの照会用に Cisco UXL Web サービスを使用します。 Cisco IP Phone Address Book Synchronizer を使用する場合は、このサービスをパブリッシャ ノード (パブリッシャ ノードを推奨) でこのサービスをアクティブ化する必要があります。Cisco IP Phone Address Book Synchronizer を使用しない場合、このサービスをアクティブ化することを推奨します。このサービスはデフォルトでは非アクティブ化されています。
Cisco Platform Administrative Web サービス	アップグレードの管理、バージョンの切り替え、操作の再開または再対処の Cisco Prime Collaboration Deployment (PCD) サーバを使用する場合は、このサービスをアクティブ化する必要があります。Platform Administrative Web サービスにより、Call Manager と Prime Collaboration Deployment (PCD) の間で通信を行うことができます。クラスタ内に複数のノードがある場合は、クラスタ内の各サーバでこのサービスをアクティブ化する必要があります。
Cisco TAPS サービス	Cisco Unified Communications Manager Auto-Register Phone Tool を使用する前に、最初のノードでこのサービスをアクティブ化する必要があります。Cisco Unified Communications Manager Auto-Register Phone Tool のダミー MAC アドレスを作成する場合、Cisco Bulk Provisioning サービスが同じノードでアクティブ化されていることを確認してください。
パフォーマンスおよびモニタリングサービス	
Cisco Serviceability Reporter	最初のノードだけでアクティブ化します。 (注) このサービスは、他のノードでアクティブ化されていても、最初のノードだけでレポートを生成します。

サービス/サブレット	アクティブ化の推奨事項
Cisco CallManager SNMP サービス	SNMP を使用する場合は、このサービスをクラスタ内のすべてのサーバでアクティブ化します。
セキュリティ サービス (Security Services)	
Cisco CTL Provider	クラスタ内のすべてのサーバでアクティブ化します。
Cisco Certificate Authority Proxy Function (CAPF)	最初のノードだけでアクティブ化します。
ディレクトリサービス	
Cisco DirSync	最初のノードだけでアクティブ化します。

IM and Presence Service のクラスタ サービス アクティベーションに関する推奨事項



注意 ある機能のいずれかのサービスを有効にする前に、その機能について IM and Presence で必要なすべての設定を行う必要があります。各 IM and Presence 機能については、関連マニュアルを参照してください。

クラスタ内でサービスを有効にする前に、マルチノード構成での IM and Presence 構成の推奨事項を示した次の表を確認してください。

表 36: IM and Presence Service アクティベーションに関する推奨事項

サービス/サブレット	推奨事項
データベースおよび管理者サービス	

サービス/サブレット	推奨事項
Cisco AXL Web Service	<p>インストール後は、すべてのクラスタノードで Cisco AXL Web サービスがデフォルトで有効になります。IM and Presence Service データベースパブリッシャノードでサービスを常にアクティベートしたままにしておくことを推奨します。これにより、AXLに依存している製品を構成できるようになります。クラスタ間通信が構成されている場合、リモートピアからの同期元として構成されたサブクラスタ内の両方のノードで、このサービスを有効にする必要があります。このサービスが両方のノードでイネーブルになっていない場合、プレゼンス機能および IM 機能はフェールオーバー時に失われます。</p> <p>必要に応じて、[Cisco Unified Serviceability] で [機能サービス (Feature Services)] の下にある特定の IM and Presence サブスクライバノードで、このサービスをアクティベートまたは非アクティベートできます。</p>
Cisco Bulk Provisioning サービス	<ul style="list-style-type: none"> • Cisco Bulk Provisioning サービスは、最初のノードだけで有効にします。 • Bulk Administration Tool (BAT) を使用してユーザを管理している場合は、このサービスを有効にする必要があります。
パフォーマンスおよびモニタリング サービス (Performance and Monitoring Services)	
Cisco Serviceability Reporter	<p>このサービスは、パブリッシャノードのみで有効にします。</p> <p>(注) このサービスは、他のノードでサービスを有効にした場合でも、必ずパブリッシャノードでレポートを生成します。</p>
IM and Presence サービス	
Cisco SIP Proxy	このサービスは、クラスタ内のすべてのノードで有効にします。
Cisco Presence Engine	このサービスは、クラスタ内のすべてのノードで有効にします。
Cisco Sync Agent	このサービスは、クラスタ内のすべてのノードで有効にします。

サービス/サブレット	推奨事項
Cisco XCP Text Conference Manager	<ul style="list-style-type: none"> • IM and Presence でチャット機能を展開する場合はこのサービスを有効にします。 • このサービスは、チャット機能を実行する各ノードで有効にします。 <p>(注) 永続的なチャット機能は、外部データベースを必要とします。永続的なチャット機能を有効にする場合、Text Conference Manager サービスを起動する前に、外部データベースも設定する必要があります。Text Conference Manager サービスは、永続的なチャット機能が有効でも外部データベースが設定されていない場合は起動しません。については、『<i>Unified Communications Manager Database Setup Guide for IM and Presence</i>』を参照してください。</p>
Cisco XCP Web Connection Manager	<ul style="list-style-type: none"> • Web クライアントを IM and Presence と統合する場合はこのサービスを有効にします。 • このサービスは、クラスタ内のすべてのノードで有効にします。
Cisco XCP Connection Manager	<ul style="list-style-type: none"> • XMPP クライアントを IM and Presence と統合する場合はこのサービスを有効にします。 • このサービスは、クラスタ内のすべてのノードで有効にします。
Cisco XCP SIP Federation Connection Manager	<p>次のいずれかの構成を展開する場合はこのサービスを有効にします。</p> <ul style="list-style-type: none"> • IM and Presence 上で SIP プロトコルを介したドメイン間フェデレーション。このサービスは、SIP フェデレーションを実行する各ノードで有効にします。 • IM and Presence Release 9.x クラスタと Cisco Unified Presence Release 8.6(x) クラスタ間のクラスタ間導入。このサービスは、Release 9.x クラスタ内のすべてのノードで有効にします。

サービス/サブレット	推奨事項
Cisco XCP XMPP Federation Connection Manager	<ul style="list-style-type: none"> • このサービスは、IM and Presence 上で XMPP プロトコルを介したドメイン間フェデレーションを展開する場合にのみ有効にします。 • このサービスは、XMPP フェデレーションを実行する各ノードで有効にします。 <p>(注) ノードで XMPP Federation Connection Manager サービスを有効にする前に、そのノードの Cisco Unified Communications Manager IM and Presence Administration で XMPP フェデレーションを有効にする必要があります。については、『<i>Unified Communications Manager Interdomain Federation for IM and Presence</i>』を参照してください。</p>
Cisco XCP Message Archiver	<ul style="list-style-type: none"> • IM and Presence でコンプライアンス機能を展開する場合はこのサービスを有効にします。 • このサービスは、IM コンプライアンス機能を実行するすべてのノードで有効にします。 <p>(注) 外部データベースを設定する前に Message Archiver を有効にしても、サービスは開始されません。また、外部データベースに到達できない場合もサービスは開始されません。については、『<i>Unified Communications Manager Database Setup Guide for IM and Presence</i>』を参照してください。</p>

サービス/サブレット	推奨事項
Cisco XCP Directory Service	<ul style="list-style-type: none"> • IM and Presence 上の XMPP クライアントを LDAP ディレクトリと統合する場合はこのサービスを有効にします。 • このサービスは、クラスタ内のすべてのノードで有効にします。 <p>(注) サードパーティ XMPP クライアント用の連絡先検索設定を行う前に Directory Service を有効にしても、サービスは開始されますが、再度停止されます。Unified Communications Manager については、『Configuration and Administration of IM and Presence Service』を参照してください。</p>
Cisco XCP Authentication Service	<ul style="list-style-type: none"> • XMPP クライアントを IM and Presence と統合する場合はこのサービスを有効にします。 • このサービスは、クラスタ内のすべてのノードで有効にします。

機能サービスのアクティブ化

Serviceability GUI の [サービスの開始 (Service Activation)] ウィンドウで、機能サービスをアクティブ化および非アクティブ化します。[サービスの開始 (Service Activation)] ウィンドウに表示されるサービスは、アクティブ化されるまで起動しません。

(ネットワーク サービスではなく) 機能サービスのみをアクティブ化および非アクティブ化することができます。必要な数のサービスを同時にアクティブ化または非アクティブ化できます。一部の機能サービスは他のサービスに依存しているため、その依存しているサービスがアクティブ化してから、該当の機能サービスがアクティブ化します。



ヒント Unified Communications Manager と IM and Presence Service のみ : [サービスの開始 (Service Activation)] ウィンドウでサービスをアクティブ化する前に、クラスタサービスをアクティブ化する際の推奨事項に関連するトピックを確認してください。

手順

ステップ 1 [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。

[サービスの開始 (Service Activation)] ウィンドウが表示されます。

ステップ 2 [サーバ (Server)] ドロップダウンリストからサーバ (ノード) を選択し、[移動 (Go)] をクリックします。

IM and Presence Service ノードから Unified Communications Manager サービスにアクセスしたり、その逆を行うことができます。リモートノードにアクセスしようとすると、次のエラーが発生する場合があります。「サーバへの接続が確立できません(リモートノードに接続できません) (Connection to the Server cannot be established (unable to connect to Remote Node))」。このエラーメッセージが表示された場合は、『*Administration Guide for Cisco Unified Communications Manager*』を参照してください。

ステップ 3 次のいずれかの操作を実行してサービスを有効または無効にします。

- a) 単一サーバで実行する必要があるデフォルト サービスをオンにするには、[デフォルトに設定 (Set to Default)] を選択します。

(注) このオプションを選択すると、単一サーバの構成に基づいてデフォルトのサービスが選択され、サービスの依存関係が確認されます。
- b) すべてのサービスを有効にするには、[すべてのサービスをチェック (Check All Services)] をオンにします。
- c) 特定のサービスを有効にするには、有効にするサービスのチェックボックスをオンにします。
- d) サービスを無効にするには、無効にするサービスのチェックボックスをオフにします。

ステップ 4 Unified Communications Manager と IM and Presence Service のみ：クラスタ構成の場合は、クラスタサービスのアクティブ化に関する推奨事項を確認してから、アクティブ化するサービスの隣にあるチェックボックスをオンにします。

ステップ 5 アクティブ化するサービスのチェックボックスをオンにした後、[保存 (Save)] をクリックします。

ヒント アクティブ化したサービスを非アクティブ化するには、非アクティブ化するサービスの隣にあるチェックボックスをオフにして、[保存 (Save)] をクリックします。

ヒント サービスの最新の状態を取得するには、[更新 (Refresh)] ボタンをクリックします。

関連トピック

[Cisco Unified Communications Manager のクラスタ サービス アクティベーションに関する推奨事項 \(252 ページ\)](#)

[IM and Presence Service のクラスタ サービス アクティベーションに関する推奨事項 \(256 ページ\)](#)

コントロールセンターまたは CLI でのサービスの開始、停止、再起動

これらのタスクを実行するために、Serviceability GUI には 2 つのコントロールセンター ウィンドウがあります。ネットワークサービスを開始、停止、および再起動するには、[コントロールセンター—ネットワークサービス (Control Center—Network Services)] ウィンドウにアクセスします。機能サービスを開始、停止、および再起動するには、[コントロールセンター - 機能サービス (Control Center—Feature Services)] ウィンドウにアクセスします。



ヒント [関連リンク (Related Links)] リストボックスと [移動 (Go)] ボタンを使用して、[コントロールセンター (Control Center)] ウィンドウと [サービスの開始 (Service Activation)] ウィンドウにナビゲートします。

コントロールセンターでのサービスの開始、停止、再起動

有用性 GUI のコントロールセンターでは、次の操作を実行できます。

- ステータスの表示
- ステータスの更新
- 特定のサーバ、またはクラスタ構成のクラスタ内のサーバに対して、機能およびネットワークサービスを開始、停止、および再起動します。

サービスが停止中の場合、サービスが停止するまで起動できないことに注意してください。



注意 Unified Communications Manager のみ：サービスを停止すると、そのサービスによって制御されるすべてのデバイスの呼処理も停止します。サービスを停止しても、IP フォンから別の IP フォンへのコールは接続されたまま、IP フォンから Media Gateway Control Protocol (MGCP) ゲートウェイへの進行中のコールも接続されたままになります。他の種類のコールはドロップされます。

手順

ステップ 1 起動/停止/再起動/更新するサービスのタイプに応じて、次のいずれかのタスクを実行します。

- [ツール (Tools)] > [コントロールセンター - 機能サービス (Control Center - Feature Services)] の順に選択します。

ヒント 機能サービスは、起動/停止/再起動する前にアクティブ化する必要があります。

- [ツール (Tools)] > [コントロールセンター - ネットワーク サービス (Control Center - Network Services)] を選択します。

ステップ 2 [サーバ (Server)] ドロップダウンリストからサーバを選択し、[移動 (Go)] をクリックします。

ウィンドウに次の項目が表示されます。

- 選択したサーバのサービス名。
- サービス グループ。
- サービス ステータス。[起動済み (Started)]、[実行中 (Running)]、[停止中 (Not Running)] など ([ステータス (Status)] カラム) 。
- サービスが実行を開始した正確な時刻 ([開始時間 (Start Time)] カラム) 。
- サービスを実行している時間 ([アップタイム (Up Time)] カラム) 。

ステップ 3 次のいずれかの操作を行います。

- 起動するサービスの横にあるオプションボタンをクリックし、[開始 (Start)] をクリックします。[ステータス (Status)] が変化し、更新されたステータスが反映されます。
- 停止するサービスの横にあるオプションボタンをクリックし、[停止 (Stop)] をクリックします。[ステータス (Status)] が変化し、更新されたステータスが反映されます。
- 再起動するサービスの横にあるオプションボタンをクリックし、[再起動 (Restart)] をクリックします。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ます。[OK] をクリックします。
- サービスの最新の状態を表示するには、[更新 (Refresh)] をクリックします。
- [サービスの開始 (Service Activation)] ウィンドウまたは他のコントロールセンター ウィンドウを表示するには、[関連リンク (Related Links)] ドロップダウンリストからオプションを選択し、[移動 (Go)] をクリックします。

コマンドライン インターフェイスを使用したサービスの開始、停止、再起動

CLI を使用して、一部のサービスを開始および停止できます。CLI で開始および停止できるサービスのリスト、およびこれらのタスクの実行方法については、『*Command Line Interface Reference Guide For Cisco ユニファイドソリューション*』を参照してください。



ヒント ほとんどのサービスは、Serviceability GUI のコントロールセンターから開始または停止する必要があります。



第 17 章

Trace

- [Trace \(265 ページ\)](#)
- [トレースの設定 \(269 ページ\)](#)

Trace

Cisco Unified Serviceability では、音声アプリケーションの問題のトラブルシューティングで利用できるトレース ツールを提供しています。Cisco Unified Serviceability は、SDI (System Diagnostic Interface) トレース、Cisco CallManager サービスおよび Cisco CTIManager サービス用の SDL (Signaling Distribution Layer) トレース (Unified Communications Manager に適用可能)、および Java アプリケーション用の Log4J トレースをサポートしています。

トレースする情報のレベルや、各トレース ファイルに含める情報の種類は、[トレース設定 (Trace Configuration)] ウィンドウを使用して指定します。

Unified Communications Manager のみ：サービスが、Cisco CallManager や Cisco CTIManager などのコール処理アプリケーションの場合、電話機やゲートウェイなどのデバイスに対してトレースを設定することができます。

Unified Communications Manager のみ：[アラーム設定] ウィンドウで、SDL トレース ログ ファイルなど、さまざまな場所にアラームを送ることができます。必要に応じて、Cisco Unified Real-Time Monitoring Tool (Unified RTMT) での警告用にトレースを設定することもできます。

さまざまなサービスに対しトレース ファイルに含める情報を設定したら、Cisco Unified Real-Time Monitoring Tool の Trace and Log Central オプションを使用して、トレース ファイルを収集および表示できます。

Cisco Unified IM and Presence Serviceability には、インスタント メッセージングおよびプレゼンス アプリケーションの問題のトラブルシューティングに利用できるトレース ツールが用意されています。Cisco Unified IM and Presence Serviceability では、次のトレースをサポートしています。

- SDI トレース
- Log4J トレース (Java アプリケーション用)

トレースする情報のレベル (デバッグレベル)、トレースする情報 (トレースフィールド)、トレースファイルに関する情報 (サービスあたりのファイル数、ファイルのサイズ、およびデータがトレースファイルに保存されている時間など) を設定することができます。1つのサービスのトレースを設定したり、そのサービスのトレース設定をクラスタ内のすべてのサーバに適用したりできます。

[アラーム設定 (Alarm Configuration)] ウィンドウでは、さまざまな場所にアラームを送ることができます。必要に応じて、IM and Presence Unified RTMT での警告用にトレースを設定することもできます。

さまざまなサービスに対しトレース ファイルに含める情報を設定したら、Unified RTMT の Trace and Log Central オプションを使用して、トレース ファイルを収集および表示できます。クラスタ内の任意の IM and Presence ノードで使用できる任意の機能またはネットワーク サービスのトレース パラメータを設定できます。[トレース設定 (Trace Configuration)] ウィンドウを使用して、問題をトラブルシューティングするためにトレースするパラメータを指定します。独自のトレース フィールドを選択する代わりに、あらかじめ決められたトラブルシューティングトレース設定を使用するには、[トラブルシューティングトレース設定 (Troubleshooting Trace Settings)] ウィンドウを使用します。



- (注) トレースをイネーブルにすると、システムのパフォーマンスが低下します。そのため、トレースは、トラブルシューティング目的でのみイネーブルにします。トレースの使用について支援が必要な場合は、Cisco Technical Assistance Center (TAC) にお問い合わせください。

トレース設定

有用性インターフェイスに表示される機能またはネットワークサービスのトレースパラメータを設定できます。クラスタがある場合は、クラスタ内の任意のサーバで使用できる機能またはネットワーク サービスに対してトレース パラメータを設定できます。[トレース設定 (Trace Configuration)] ウィンドウを使用して、問題をトラブルシューティングするためにトレースするパラメータを指定します。

トレースする情報のレベル (デバッグレベル)、トレースする情報 (トレースフィールド)、およびトレースファイルに関する情報 (サービスごとのファイル数、ファイルサイズ、トレースファイルにデータが保存された時間など) を設定できます。クラスタがある場合は、1つのサービスのトレースを設定するか、またはそのサービスのトレース設定をクラスタ内のすべてのサーバに適用することができます。

独自のトレースフィールドを選択する代わりに、あらかじめ決められたトラブルシューティングトレース設定を使用するには、[トラブルシューティングトレース (Troubleshooting Trace)] ウィンドウを使用します。トレースのトラブルシューティングの詳細については、「トレース設定」を参照してください。

さまざまなサービスに対しトレース ファイルに含める情報を設定したら、Unified RTMT の Trace and Log Central オプションを使用して、トレース ファイルを収集できます。トレース収集に関する詳細については、「トレース収集」を参照してください。

トレース設定

[トラブルシューティング トレース設定 (Troubleshooting Trace Settings)] ウィンドウでは、事前に設定されたトラブルシューティング トレース設定に設定するサービスを選択できます。このウィンドウでは、1つ以上のサービスを選択し、これらのサービスの設定を、事前に設定されたトレース設定に変更できます。クラスタがある場合、クラスタ内の異なるサーバ上のサービスを選択して、そのサービスのトレース設定を事前に設定されたトレース設定に変更することができます。1台のサーバの特定のアクティブ化されたサービス、サーバのすべてのアクティブ化されたサービス、クラスタ内のすべてのサーバの特定のアクティブ化されたサービス、クラスタ内のすべてのサーバのすべてのアクティブ化されたサービスを選択できます。このウィンドウでは、非アクティブなサーバの横に [N/A] と表示されます。



- (注) 機能またはネットワーク サービスの事前に決定されたトラブルシューティング トレース設定には、SDL、SDI、および Log4j トレース設定があります。トラブルシューティング トレース設定が適用される前に、元のトレース設定がバックアップされます。トラブルシューティング トレース設定をリセットすると、元のトレース設定が復元されます。

トラブルシューティング トレース設定をサービスに適用した後で [トラブルシューティング トレース設定 (Troubleshooting Trace Settings)] ウィンドウを開くと、トラブルシューティング用に設定したサービスがチェック付きで表示されます。[トラブルシューティング トレース設定 (Troubleshooting Trace Settings)] ウィンドウでは、トレース設定を元の設定にリセットできます。

トラブルシューティング トレース設定をサービスに適用すると、トラブルシューティング トレースがそのサービスに設定されたことを示すメッセージが [トレース設定 (Trace Configuration)] ウィンドウに表示されます。サービスの設定をリセットする場合は、[関連リンク (Related Links)] ドロップダウンリストボックスから、[トラブルシューティング トレース設定 (Troubleshooting Trace Settings)] オプションを選択できます。指定したサービスの [トレース設定 (Trace Configuration)] ウィンドウでは、すべての設定が読み取り専用として表示されます。ただし、最大ファイル数など、トレース出力設定の一部のパラメータを除きます。これらのパラメータは、トラブルシューティング トレース設定を適用した後も変更できます。

トレース収集

各種サービス トレースやその他のログファイルを収集、表示、および zip 圧縮するには、Trace and Log Central (Cisco Unified Real-Time Monitoring Tool のオプション) を使用します。Trace and Log Central オプションを使用すると、SDL/SDI トレース、アプリケーションログ、システムログ (イベントビューアアプリケーションログ、セキュリティログ、システムログなど)、クラッシュ ダンプ ファイルを収集できます。



ヒント 収集されたトレースファイルを表示するために、収集したトレースファイルを表示するために Windows NotePad を使用しないでください。これは、Windows NotePad で改行が正しく表示されないためです。



(注) Unified Communications Manager のみ：暗号化をサポートするデバイスでは、Secure Real-time Transport Protocol (SRTP) のセキュア キー関連情報はトレース ファイルに表示されません。

トレース収集の詳細情報については、『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。

着信側トレース

着信側トレースでは、トレースする電話番号または電話番号のリストを設定することができます。セッショントレース ツールを使用してコールのオンデマンド トレースを要求できます。

詳細については、『Cisco Unified Real-Time Monitoring Tool Administration Guide』を参照してください。

トレース設定のセットアップ

次の手順は、有用性インターフェイスで機能およびネットワークサービスのトレースを設定および収集する手順の概要を示しています。

手順

- ステップ 1** 次のいずれかの手順を実行して、TLC Throttling CPU Goal および TLC Throttling IOWait Goal サービス パラメータ (Cisco RIS Data Collector サービス) の値を設定します。
- Cisco Unified Communications Manager Administration および Cisco Unified IM and Presence : システム > サービス パラメータ を選択し、TLC Throttling CPU Goal および TLC Throttling IOWait Goal サービス パラメータ (Cisco RIS Data Collector サービス) の値を設定します。
 - Cisco Unity Connection のみ : Cisco Unity Connection Administration で [システム設定 (System Settings)] > [サービス パラメータ (Service Parameters)] を選択し、TLC Throttling CPU Goal および TLC Throttling IOWait Goal サービス パラメータ (Cisco RIS Data Collector サービス) の値を設定します。
- ステップ 2** トレースを収集するサービスのトレース設定を行います。クラスタがある場合、1 台のサーバ、またはクラスタ内のすべてのサーバに対してサービスのトレースを設定できます。
- トレース設定を行う場合、デバッグ レベルとトレース フィールドを選択してトレース ログに含める情報を選択します。

サービスで事前に設定されているトレースを実行する場合は、これらのサービスのトラブルシューティング トレースを設定します。

- ステップ 3** ローカル PC に Cisco Unified Real-Time Monitoring Tool をインストールします。
- ステップ 4** 監視されているトレースファイル内に指定された検索文字列が存在するときにアラームを生成する場合は、Unified RTMT の LogFileSearchStringFound アラートを有効にします。
- LogFileSearchStringFound アラームは LpmTctCatalog にあります。[アラーム (Alarms)] > [定義 (Definitions)] を選択します。[アラームの検索場所 (Find alarms where)] ドロップダウン リスト ボックスで [システムアラームカタログ (System Alarm Catalog)] を選択し、[等しい (Equals)] ドロップダウン リスト ボックスで [LpmTctCatalog] を選択します。
- ステップ 5** CriticalServiceDownand CodeYellow など、アラートのトレースを自動的にキャプチャする場合は、Unified RTMT の特定のアラートの [アラート/プロパティの設定 (Set Alert/Properties)] ダイアログボックスで [トレースダウンロードのイネーブル化 (Enable Trace Download)] チェックボックスをオンにし、ダウンロードを実行する頻度を設定します。
- ステップ 6** トレースを収集します。
- ステップ 7** 適切なビューアでログ ファイルを表示します。
- ステップ 8** トラブルシューティング トレースをイネーブルにすると、トレース設定サービスがリセットされて、元の設定に戻ります。

(注) トラブルシューティング トレースを長時間イネーブルのままにすると、トレースファイルのサイズが大きくなり、サービスのパフォーマンスに影響が生じるおそれがあります。

トレースの設定

ここでは、トレース設定の構成について説明します。



- (注) トレースをイネーブルにすると、システムのパフォーマンスが低下します。そのため、トレースは、トラブルシューティング目的でのみイネーブルにします。トレースの使用について支援が必要な場合は、テクニカル サポート チームにお問い合わせください。

トレース パラメータの設定

ここでは、Serviceability GUI で管理する機能サービスとネットワーク サービスのトレース パラメータを設定する方法について説明します。



ヒント Cisco Unity Connection では、Cisco Unified Serviceability および Cisco Unity Connection Serviceability でトレースを実行して Cisco Unity Connection の問題をトラブルシューティングする必要がある場合があります。Cisco Unity Connection Serviceability でトレースを実行する方法については、『Cisco Unity Connection Serviceability アドミニストレーションガイド』を参照してください。

手順

ステップ 1 [トレース (Trace)] > [設定 (Configuration)] を選択します。

[トレース設定 (Trace Configuration)] ウィンドウが表示されます。

ステップ 2 [サーバ (Server)] ドロップダウンリストボックスから、トレースを設定するサービスを実行しているサーバを選択し、[移動 (Go)] をクリックします。

ステップ 3 [サービスグループ (Service Group)] ドロップダウンリストボックスから、トレースを設定するサービスのサービスグループを選択し、[移動 (Go)] をクリックします。

ヒント 「トレース設定のサービスグループ」の表に、[サービスグループ (Service Group)] ドロップダウンリストボックスに表示されるオプションに対応するサービスとトレースライブラリの一覧を示します。

ステップ 4 [サービス (Service)] ドロップダウンリストボックスからトレースを設定するサービスを選択し、[移動 (Go)] をクリックします。

ドロップダウンリストボックスには、アクティブなサービスと非アクティブのサービスが表示されます。

ヒント Cisco Unity Connection のみ: Cisco CallManager および CTIManager サービスの場合は、SDL トレースパラメータを設定できます。設定を行うには、いずれかのサービスの [トレース設定 (Trace Configuration)] ウィンドウを開き、[関連リンク (Related Links)] ドロップダウンリストボックスの横にある [移動 (Go)] ボタンをクリックします。

サービスのトラブルシューティングトレースを設定した場合は、トラブルシューティングトレース機能が設定されていることを示すメッセージがウィンドウの上部に表示されます。これは、トレースを除いて、[トレース設定 (Trace Configuration)] ウィンドウのすべてのフィールドが無効になっていることを意味します。出力設定。[トレース出力設定 (Trace Output Settings)] を設定するには、ステップ 11 に進みます。トラブルシューティングトレースをリセットするには、トラブルシューティングトレース設定のセットアップを参照してください。

選択したサービスのトレースパラメータが表示されます。また、[すべてのノードに適用 (Apply to All Nodes)] チェックボックスが表示されます (Cisco Unified Communications Manager のみ)。

ステップ 5 Unified Communications Manager および IM and Presence のみ: クラスタをサポートしている設定の場合は、必要に応じて [すべてのノードに適用 (Apply to All Nodes)] チェックボックスを

オンにして、クラスタ内のすべてのサーバにサービスのトレース設定またはトレースライブラリを適用できます。

- ステップ 6** **トレースオン**チェックボックスをオンにします。
- ステップ 7** Cisco Unity Connection のみ: SDL トレースパラメータを設定する場合は、ステップ10に進みます。
- ステップ 8** 「デバッグトレースレベルの設定」の記述に従って、トレースする情報のレベルを[デバッグトレースレベル (Debug Trace Level)]リストボックスから選択します。
- ステップ 9** 選択したサービスの[トレースフィールド (Trace Fields)]チェックボックス (たとえば、[Cisco Log Partition Monitoring Toolトレースフィールド (Cisco Log Partition Monitoring Tool Trace Fields)]) をオンにします。
- ステップ 10** アクティブ化するトレースを指定できるトレース設定がサービスに複数存在しない場合は、[すべてのトレースをイネーブル化 (Enable All Trace)]チェックボックスをオンにします。選択したサービスに複数のトレース設定がある場合は、[トレース(Trace)]フィールドの説明に従って、有効にする[トレース(trace)]チェックボックスの横にあるチェックボックスをオンにします。
- ステップ 11** トレースファイルの数とサイズを制限するには、トレース出力設定を指定します。説明については、「トレース出力の設定」を参照してください。
- ステップ 12** トレースパラメータの設定を保存するには、[保存 (Save)]ボタンをクリックします。

トレース設定に加えた変更は、Cisco Messaging Interface 以外のすべてのサービスに即座に反映されます (Unified Communications Manager のみ)。Cisco Messaging Interface のトレースの設定変更は、3 ~ 5 分で有効になります。

(注) デフォルトを設定するには、[デフォルトの設定 (Set Default)]ボタンをクリックします。

トレース設定でのサービスグループ

次の表に、[トレース設定 (Trace Configuration)] ウィンドウの [サービスグループ (Service Group)] ドロップダウンリストボックスに表示されるオプションに対応するサービスとトレースライブラリの一覧を示します。

表 37: トレース設定でのサービスグループ

サービスグループ	サービスとトレースライブラリ	注記
Unified Communications Manager CM サービス (CM Services)	<ul style="list-style-type: none"> • Cisco CTIManager • Cisco CallManager • Cisco CallManager Cisco IP 電話サービス • Cisco DHCP Monitor サービス • Cisco Dialed Number Analyzer • Cisco Dialed Number Analyzer Server • Cisco Extended Functions、Cisco Extension Mobility • Cisco Extension Mobility アプリケーション • Cisco IP Voice Media Streaming App • Cisco Messaging Interface • Cisco TFTP • Cisco Unified Mobile Voice Access Service 	CM サービスグループのほとんどのサービスでは、サービスのすべてのトレースを有効化する代わりに、特定のコンポーネントのトレースを実行することができます。[トレース (Trace)] フィールドの説明は、特定のコンポーネントのトレースを実行できるサービスを示します。
Unified Communications Manager CTI サービス	<ul style="list-style-type: none"> • Cisco IP Manager Assistant • Cisco Web Dialer Web Service 	これらのサービスでは、サービスに対してすべてのトレースを有効化する代わりに、特定のコンポーネントのトレースを実行できます。トレースフィールドの説明を参照してください。

サービスグループ	サービスとトレースライブラリ	注記
Unified Communications Manager CDR サービス	<ul style="list-style-type: none"> • Cisco Unified Communications Manager CDR Analysis and Reporting Scheduler • Cisco Unified Communications Manager CDR Analysis and Reporting Web Service • Cisco CDR Agent • Cisco CDR Repository Manager 	<p>特定のコンポーネントのトレースを実行する代わりに、各サービスのすべてのトレースをイネーブルにします。</p> <p>Cisco CDR Analysis and Reporting では、ストアードプロシージャを呼び出すレポートが実行されると、ストアードプロシージャのロギングが開始される前に、CDR Analysis and Reporting が [トレース設定] ウィンドウの CDR Analysis and Reporting Scheduler サービスおよび CDR Analysis and Reporting Web サービスの設定されたデバッグ トレース レベルを確認します。事前生成レポートの場合は、Cisco Unified Communications Manager CDR Analysis and Reporting が Cisco Unified Communications Manager CDR Analysis and Reporting Scheduler サービスのレベルをチェックします。オンデマンド レポートの場合は、Cisco Unified Communications Manager CDR Analysis and Reporting が Cisco Unified Communications Manager CDR Analysis and Reporting Web Service のレベルをチェックします。[Debug Trace Level] ドロップダウン リスト ボックスから [Debug] を選択した場合、ストアードプロシージャのロギングがイネーブルにされ、ドロップダウン リスト ボックスで別のオプションを選択するまで続行されます。以下の Cisco Unified Communications Manager CDR Analysis and Reporting レポートでは、ストアードプロシージャのロギングが使用されます。ゲートウェイ使用状況レポート、ルートおよび回線グループ使用状況レポート、ルートまたはハント リスト使用状況レポート、ルート パターンまたはハントパイロット使用状況レポート、会議コール詳細レポート、会議コール要約レポート、会議ブリッジ使用状況レポート、ボイス メッセージ使用状況レポート、CDR 検索レポート。</p>

サービスグループ	サービスとトレースライブラリ	注記
IM and Presence サービス	<ul style="list-style-type: none"> • Cisco Client Profile Agent • Cisco Config Agent • Cisco Intercluster Sync Agent • Cisco Login Datastore • Cisco OAM Agent • Cisco Presence Datastore • Cisco Presence Engine • Cisco IM and Presence Data Monitor • Cisco Route Datastore • Cisco SIP Proxy • Cisco SIP Registration Datastore • Cisco Server Recovery Manager • Cisco Sync Agent • Cisco XCP Authentication Service • Cisco XCP Config Manager • Cisco XCP Connection Manager • Cisco XCP Directory Service • Cisco XCP Message Archiver • Cisco XCP Router • Cisco XCP SIP Federation Connection Manager • Cisco XCP Text Conference Manager • Cisco XCP Web Connection Manager • Cisco XCP XMPP Federation Connection Manager 	<p>これらのサービスの説明については、Cisco Unified IM and Presence Serviceability の機能とネットワーク サービスに関連するトピックを参照してください。</p> <ul style="list-style-type: none"> • これらのサービスでは、特定のコンポーネントのトレースを実行する代わりに、このサービスのすべてのトレースをイネーブルにする必要があります。

サービスグループ	サービスとトレースライブラリ	注記
データベースおよび管理者サービス	<p>Unified Communications Manager および Cisco Unity Connection:</p> <ul style="list-style-type: none"> • Cisco AXL Web Service • Cisco CCM DBL Web Library • Cisco CCMAdmin Web Service • Cisco CCMUser Web Service • Cisco Database Layer Monitor • Cisco UXL Web サービス <p>Unified Communications Manager</p> <ul style="list-style-type: none"> • Cisco Bulk Provisioning サービス • Cisco GRT Communications Web サービス • Cisco Role-based Security • Cisco TAPS サービス • Cisco Unified Reporting Web Service <p>IM and Presence Service :</p> <ul style="list-style-type: none"> • Cisco AXL Web Service • Cisco Bulk Provisioning サービス • Cisco CCMUser Web Service • Cisco Database Layer Monitor • Cisco GRT Communications Web サービス • Cisco IM and Presence Admin • Cisco Unified Reporting Web Service • Platform Administrative Web サービス 	<p>Cisco CCM DBL Web Library オプションを選択すると、Java アプリケーションのデータベース アクセスのトレースがアクティブ化されます。C++ アプリケーションのデータベースアクセスの場合は、<code>cisco Extended Functions trace</code> フィールドの説明に従って、Cisco Database Layer Monitor のトレースを有効にします。</p> <p>Unified Communications Manager をサポートする Cisco Role-based Security オプションを選択すると、ユーザ ロールの許可に対するトレースが有効となります。</p> <p>データベースおよび管理者サービスグループのほとんどのサービスでは、特定のコンポーネントのトレースをイネーブルにするのではなく、サービスまたはライブラリのすべてのトレースをイネーブルにします。Cisco Database Layer Monitor の場合、特定のコンポーネントのトレースを実行できます。</p> <p>(注) サービスのロギングの制御は、Cisco Unified IM and Presence Serviceability の UI で実行できます。ログレベルを変更するには、[システムサービス (System Services)] グループと [Cisco CCMService Webサービス (Cisco CCMService Web Service)] を選択します。</p>

サービスグループ	サービスとトレースライブラリ	注記
パフォーマンスおよびモニタリングサービス (Performance and Monitoring Services)	Unified Communications Manager および Cisco Unity Connection: <ul style="list-style-type: none"> • Cisco AMC Service • Cisco CCM NCS Web Library • CCM PD Web サービス • Cisco CallManager SNMP サービス • Cisco Log Partition Monitoring Tool • Cisco RIS Data Collector • Cisco RTMT Web Service • Cisco Audit Event Service • Cisco RisBean Library Unified Communications Manager : <ul style="list-style-type: none"> • Cisco CCM PD Web サービス IM and Presence Service : <ul style="list-style-type: none"> • Cisco AMC Service • Cisco Audit Event Service • Cisco Log Partition Monitoring Tool • Cisco RIS Data Collector • Cisco RTMT Web Service • Cisco RisBean Library 	Cisco CCM NCS Web Library オプションを選択すると、Java クライアントのデータベース変更通知のトレースがアクティブ化されます。 Cisco Unity RTMT Web サービス オプションを選択すると、Unity RTMT サブプレットのトレースがアクティブ化されます。このトレースを実行すると、Unity RTMT クライアント クエリーのサーバ側のログが作成されます。
Unified Communications Manager セキュリティサービス (Security Services)	<ul style="list-style-type: none"> • Cisco CTL Provider • Cisco Certificate Authority Proxy Function • シスコ信頼検証サービス 	特定のコンポーネントのトレースを実行する代わりに、各サービスのすべてのトレースをイネーブルにします。
Unified Communications Manager ディレクトリサービス	Cisco DirSync	特定のコンポーネントのトレースを実行する代わりに、このサービスのすべてのトレースをイネーブルにします。

サービスグループ	サービスとトレースライブラリ	注記
バックアップおよび復元サービス	<ul style="list-style-type: none"> • Cisco DRF Local • Unified Communications Manager および Cisco Unity Connection のみ : Cisco DRF Master 	<p>特定のコンポーネントのトレースを実行する代わりに、各サービスのすべてのトレースをイネーブルにします。</p>
System Services	<p>Unified Communications Manager :</p> <ul style="list-style-type: none"> • Cisco CCMRealm Web Service • Cisco CCMService Web Service • Cisco Common User Interface • Cisco Trace Collection Service <p>IM and Presence Service :</p> <ul style="list-style-type: none"> • Cisco CCMService Web Service • Cisco Trace Collection Service 	<p>Cisco CCMRealm Web Service オプションを選択すると、ログイン認証のトレースがアクティブ化されます。</p> <p>Cisco Common User Interface オプションを選択すると、複数のアプリケーションが使用する共通コードのトレースがアクティブ化されます。たとえば、Cisco Unified Operating System Administration や Cisco Unified Serviceability などが該当します。</p> <p>Cisco CCMService Web Service オプションを選択すると、Cisco Unified Serviceability の Web アプリケーション (GUI) のトレースがアクティブ化されます。</p> <p>特定のコンポーネントのトレースを実行する代わりに、各オプションまたはサービスのすべてのトレースを有効化します。</p>
SOAP サービス	<ul style="list-style-type: none"> • CiscoSOAP Web サービス • CiscoSOAPMessage サービス 	<p>Cisco SOAP Web Service オプションを選択すると、AXL Serviceability API のトレースがアクティブ化されます。</p> <p>特定のコンポーネントのトレースを実行する代わりに、このサービスのすべてのトレースをイネーブルにします。</p>
プラットフォームサービス	Cisco Unified OS Admin Web Service	<p>Cisco Unified OS Admin Web Service は Cisco Unified Operating System Administration をサポートしています。これは、証明書管理、バージョンの設定、および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関連の機能を管理する Web アプリケーションです。</p> <p>特定のコンポーネントのトレースを実行する代わりに、このサービスのすべてのトレースをイネーブルにします。</p>

デバッグトレースレベルの設定

次の表に、サービスのデバッグトレースレベル設定について説明します。

表 38: サービスのデバッグトレースレベル

レベル	説明
エラー (Error)	アラーム状態およびイベントをトレースします。異常なパスで生成されたすべてのトレースに使用します。最小のCPU サイクル数を使用します。
Special	すべてのエラー状態と、プロセスおよびデバイスの初期化メッセージをトレースします。
状態遷移 (State Transition)	すべての特殊条件と、通常運用中に発生するサブシステムの状態遷移をトレースします。コール処理イベントをトレースします。
重大 (Significant)	通常運用時に発生するすべての状態遷移条件とメディアレイヤイベントをトレースします。
入口/出口	(注) すべてのサービスがこの追跡レベルを使用するわけではありません。 重要なすべての状態と、ルーチンの開始および終了点をトレースします。
任意 (Arbitrary)	すべての開始および終了状態と、低レベルのデバッグ情報をトレースします。
詳細	すべての任意の条件と、詳細なデバッグ情報をトレースします。

次の表に、servlet のデバッグトレースレベル設定について説明します。

表 39: servlet のデバッグトレースレベル

レベル	説明
[致命的 (Fatal)]	アプリケーションが中断する可能性がある重大なエラーイベントをトレースします。
エラー (Error)	アラーム状態およびイベントをトレースします。異常なパスで生成されたすべてのトレースに使用します。
[警告 (Warn)]	損害が発生する可能性がある状況をトレースします。

レベル	説明
[情報 (Info)]	サブレットの問題の多数をトレースし、システムパフォーマンスに最小限の影響を与えます。
[デバッグ (Debug)]	通常運用時に発生するすべての状態遷移条件とメディアレイヤ イベントをトレースします。 すべてのロギングを有効にするトレース レベル。

トレース フィールドの説明

一部のサービスでは、サービスのすべてのトレースをイネーブルにする代わりに、特定のコンポーネントのトレースをアクティブ化できます。次のリストに、特定のコンポーネントのトレースをアクティブにできるサービスを示します。いずれかの相互参照をクリックすると該当するセクションに移動し、サービスの各トレースフィールドの説明が表示されます。サービスが次のリストにない場合、[トレース設定 (Trace Configuration)]ウィンドウにそのサービスの [すべてのトレースをイネーブル化 (Enable All Trace)]チェックボックスが表示されます。

以下のサービスは、Unified Communications Manager および Cisco Unity Connection で利用することができます。

- Database Layer Monitor のトレース フィールド
- Cisco RIS Data Collector のトレース フィールド

以下のサービスは、Unified Communications Manager で利用することができます。

- Cisco CallManager SDI のトレース フィールド
- Cisco CallManager SDL のトレース フィールド
- Cisco CTIManager SDL のトレース フィールド
- Cisco Extended Functions のトレース フィールド
- Cisco エクステンション モビリティのトレース フィールド
- Cisco IP Manager Assistant のトレース フィールド
- Cisco IP Voice Media Streaming App のトレース フィールド
- Cisco TFTP のトレース フィールド
- Cisco WebDialer Web サービスのトレース フィールド

Database Layer Monitor のトレース フィールド

次の表に、Cisco Database Layer Monitor のトレース フィールドを示します。The Cisco Database Layer Monitor サービスは、Unified Communications Manager および Cisco Unity Connection をサポートします。

表 40: Cisco Database Layer Monitor のトレースのフィールド

フィールド名	説明
DB ライブラリ トレースのイネーブル化 (Enable DB Library Trace)	C++アプリケーションのデータベースライブラリのトレースをアクティブ化します。
サービスのトレースのイネーブル化 (Enable Service Trace)	サービスのトレースをアクティブ化します。
DB変更通知のトレースのイネーブル化 (Enable DB Change Notification Trace)	C++アプリケーションのデータベース変更通知トレースを有効にします。
単体試験のトレースのイネーブル化 (Enable Unit Test Trace)	このチェックボックスはオンにしないでください。デバッグ目的でシスコのエンジニアが使用します。

Cisco RIS Data Collector のトレースのフィールド

次の表に、Cisco RIS Data Collector のトレース フィールドを示します。Cisco RIS Data Collector サービスは、Unified Communications Manager および Cisco Unity Connectionをサポートします。

表 41: Cisco RIS Data Collector のトレースのフィールド

フィールド名	説明
RISDC のトレースのイネーブル化 (Enable RISDC Trace)	RIS データ コレクタ サービス (RIS) の RISDC スレッドのトレースをアクティブ化します。
システムアクセスのトレースのイネーブル化 (Enable System Access Trace)	RIS データ コレクタのシステム アクセス ライブラリのトレースをアクティブ化します。
リンクサービスのトレースのイネーブル化 (Enable Link Services Trace)	RIS データ コレクタのリンク サービス ライブラリのトレースをアクティブ化します。
RISDCアクセスのトレースのイネーブル化 (Enable RISDC Access Trace)	RIS データ コレクタの RISDC アクセス ライブラリのトレースをアクティブ化します。
RISDB のトレースのイネーブル化 (Enable RISDB Trace)	RIS データ コレクタの RISDB ライブラリのトレースを有効にします。
PIのトレースのイネーブル化 (Enable PI Trace)	RIS データ コレクタの PI ライブラリのトレースを有効にします。
XML のトレースのイネーブル化 (Enable XML Trace)	RIS データ コレクタ サービスの入出力 XML メッセージのトレースを有効にします。

フィールド名	説明
Perfmon ロガーのトレースのイネーブル化 (Enable Perfmon Logger Trace)	RIS データ コレクタの perfmon データ ロギングをトラブルシューティングするためのトレースを有効にします。ログファイル、記録されたカウンタの総数、アプリケーションおよびシステムカウンタとインスタンスの名前、プロセスとスレッドの CPU パーセンテージの計算、ログファイルのロールオーバーと削除の発生をトレースするために使用します。

Cisco CallManager SDI のトレース フィールド

次の表では、Cisco CallManager SDI トレースフィールドについて説明します。Cisco CallManager サービスは、Unified Communications Manager をサポートします。

表 42: Cisco CallManager SDI のトレース フィールド

フィールド名	説明
H245 メッセージトレースの有効化	H245 メッセージのトレースをアクティブ化します。
DT-24+/DE-30+のトレースのイネーブル化 (Enable DT-24+/DE-30+ Trace)	DT-24+/DE-30+ デバイス トレースの ISDN タイプのロギングをアクティブ化します。
PRIのトレースのイネーブル化 (Enable PRI Trace)	一次群速度インターフェイス (PRI) デバイスのトレースをアクティブ化します。
ISDN変換のトレースの有効化 (Enable ISDN Translation Trace)	ISDN メッセージトレースをアクティブにします。通常のデバッグに使用します。
H225 & ゲートキーパートレースの有効化	H.225 デバイスのトレースをアクティブ化します。通常のデバッグに使用します。
Enable Miscellaneous Trace	各種デバイスのトレースをアクティブ化します。 (注) 通常のシステム操作時には、このチェックボックスをオンにしないでください。
会議ブリッジのトレースの有効化 (Enable Conference Bridge Trace)	会議ブリッジのトレースをアクティブ化します。通常のデバッグに使用します。

フィールド名	説明
保留音のトレースのイネーブル化 (Enable Music on Hold Trace)	保留音 (MOH) デバイスのトレースをアクティブにします。Unified Communications Manager への登録、Unified Communications Manager への登録解除、リソース割り当ての成功または失敗など、MOH デバイスのステータスのトレースのために使用されます。
Unified CM リアルタイム情報サーバのトレースのイネーブル化 (Enable Unified CM Real-Time Information Server Trace)	Real-time Information Server が使用する Unified Communications Manager のリアルタイム情報トレースを有効化します。
SIP スタックのトレースのイネーブル化 (Enable SIP Stack Trace)	SIP スタックのトレースをアクティブ化します。デフォルトではイネーブルになっています。
アナunciエータのトレースのイネーブル化 (Enable Annunciator Trace)	Cisco Unified Communications Manager が、Cisco Unified IP Phone、ゲートウェイ、およびその他の設定可能なデバイスへ、録音済みの音声案内 (.wav ファイル) とトーンを再生できるようにするために、Cisco IP Voice Media Streaming Application サービスを使用する SCCP デバイスである Annunciator のトレースを有効化します。
CDR のトレースのイネーブル化 (Enable CDR Trace)	CDR のトレースをアクティブ化します。
アナログ トランクのトレースのイネーブル化 (Enable Analog Trunk Trace)	すべてのアナログ トランク (AT) ゲートウェイのトレースをアクティブ化します。
すべての電話機のトレースのイネーブル化 (Enable All Phone Device Trace)	電話機のトレースをアクティブ化します。トレース情報にはソフトフォンデバイスが含まれます。通常のデバッグに使用します。
MTP のトレースのイネーブル化 (Enable MTP Trace)	メディア ターミネーション ポイント (MTP) デバイスのトレースをアクティブ化します。通常のデバッグに使用します。
すべてのゲートウェイトレースのイネーブル化 (Enable All Gateway Trace)	すべてのアナログおよびデジタルゲートウェイのトレースをアクティブ化します。
転送と各種のトレースのイネーブル化 (Enable Forward and Miscellaneous Trace)	別のチェックボックスで対象にされていないコール転送およびすべてのサブシステムのトレースをアクティブ化します。通常のデバッグに使用します。

フィールド名	説明
MGCPのトレースのイネーブル化 (Enable MGCP Trace)	メディア ゲートウェイ コントロール プロトコル (MGCP) デバイスのトレースをアクティブ化します。通常のデバッグに使用します。
メディアリソースマネージャのトレースのイネーブル化 (Enable Media Resource Manager Trace)	メディア リソース マネージャ (MRM) のアクティビティのトレースをアクティブ化します。
SIPコール処理トレースの有効化 (Enable SIP Call Processing Trace)	SIP コール処理のトレースを有効化します。
Enable SCCP Keep Alive Trace	Cisco CallManager トレースの SCCP キープアライブトレース情報のトレースをアクティブ化します。各 SCCP デバイスは30秒ごとにキープアライブメッセージをレポートし、各キープアライブメッセージは3行のトレース データを作成するため、このチェックボックスがオンの場合大量のトレース データが生成されます。
Enable SIP Keep Alive (REGISTER Refresh) Trace	Cisco CallManager トレースの SIP キープアライブ (REGISTER Refresh) トレース情報のトレースをアクティブ化します。各 SIP デバイスは2秒ごとにキープアライブメッセージをレポートし、各キープアライブメッセージは複数行のトレース データを作成するため、このチェックボックスがオンの場合大量のトレース データが生成されます。

Cisco CallManager SDL のトレース フィールド

次の表で、Cisco CallManager SDL のトレース フィールド設定について説明します。Cisco CallManager サービスは、Unified Communications Manager をサポートします。



- (注) シスコのエンジニアから指示された場合を除き、デフォルト設定を使用することを推奨します。

表 43: Cisco CallManager SDL の設定に対するトレース フィルタの設定

設定名	説明
すべてのレイヤ1トレースのイネーブル化。 (Enable all Layer 1 traces.)	レイヤ1のトレースをアクティブ化します。

設定名	説明
詳細なレイヤ1のトレースのイネーブル化。 (Enable detailed Layer 1 traces.)	詳細なレイヤ1のトレースをアクティブ化します。
すべてのレイヤ2トレースのイネーブル化。 (Enable all Layer 2 traces.)	レイヤ2のトレースをアクティブ化します。
レイヤ2インターフェイストレースを有効にします。	レイヤ2インターフェイストレースをアクティブ化します。
レイヤ2TCPのトレースのイネーブル化。 (Enable Layer 2 TCP trace.)	レイヤ2 伝送制御プログラム (TCP) のトレースをアクティブ化します。
詳細なダンプレイヤ2トレースを有効にします。	ダンプレイヤ2の詳細なトレースをアクティブ化します。
すべてのレイヤ3トレースのイネーブル化。 (Enable all Layer 1 traces.)	レイヤ3のトレースをアクティブ化します。
すべてのコール制御のトレースのイネーブル化。 (Enable all call control traces.)	コール制御のトレースをアクティブにします。
各種のポーリングのトレースのイネーブル化。 (Enable miscellaneous polls trace.)	さまざまなポーリングに対するトレースをアクティブ化します。
各種のトレース(データベース信号)のイネーブル化。 (Enable miscellaneous trace (database signals).)	データベースの信号のようなさまざまなトレースをアクティブ化します。
メッセージ変換信号トレースを有効にします。	メッセージ変換信号のトレースをアクティブにします。
UUIEの出力のトレースのイネーブル化。 (Enable UUIE output trace.)	ユーザ間の情報要素 (UUIE) 出力のトレースをアクティブにします。
ゲートウェイ信号トレースを有効にします。	ゲートウェイ信号のトレースをアクティブにします。
CTIのトレースのイネーブル化。 (Enable CTI trace.)	CTIのトレースをアクティブ化します。
ネットワークサービスのデータのトレースのイネーブル化 (Enable network service data trace)	ネットワークサービスのデータのトレースをアクティブ化します。
ネットワークサービスのイベントのトレースのイネーブル化 (Enable network service event trace)	ネットワークサービスのイベントのトレースをアクティブ化します。
ICCP 管理トレースの有効化	ICCP 管理のトレースをアクティブ化します。

設定名	説明
デフォルトのトレースのイネーブル化 (Enable default trace)	デフォルトのトレースをアクティブ化します。

次の表で、Cisco CallManager SDL の設定特性について説明します。

表 44 : Cisco CallManager SDL の設定に対するトレースの特性

特性	説明
SDLリンクステートのトレースのイネーブル化。(Enable SDL link states trace.)	クラスタ内通信プロトコル (ICCP) リンクステートのトレースをアクティブ化します。
低レベルのSDLのトレースのイネーブル化。(Enable low-level SDL trace.)	低レベルのSDLのトレースをアクティブ化します。
SDL リンクポーリングトレースを有効にします。	ICCPリンクのポーリングのトレースをアクティブ化します。
SDLリンクメッセージのトレースのイネーブル化。(Enable SDL link messages trace.)	ICCP未処理メッセージのトレースをアクティブ化します。
信号データダンプトレースを有効にします。	信号データのダンプに対するトレースをアクティブ化します。
関連タグのマッピングのトレースのイネーブル化。(Enable correlation tag mapping trace.)	関連タグのマッピングに対するトレースをアクティブ化します。
SDLプロセスの状態のトレースのイネーブル化。(Enable SDL process states trace.)	SDLプロセス状態のトレースを有効にします。
SDLのprettyプリントのトレースの無効化。(Disable pretty print of SDL trace.)	SDLのprettyプリントに対するトレースを無効化します。prettyプリントでは、後処理を実行しないでトレースファイルにタブとスペースを追加します。
SDL TCP イベントトレースを有効にします。	SDL TCP イベントのトレースをアクティブ化します。

Cisco CTIManager SDL のトレース フィールド

次の表で、Cisco CTIManager SDL 設定のトレース フィルタの設定について説明します。Cisco CTIManager サービスは Unified Communications Manager をサポートします。



ヒント シスコのエンジニアから指示された場合を除き、デフォルト設定を使用することを推奨します。



ヒント [サービスグループ (Service Groups)] ドロップダウン リスト ボックスから CTIManager サービスを選択すると、[トレース設定 (Trace Configuration)] ウィンドウにこのサービスの SDI トレースが表示されます。Cisco CTI Manager サービスに対する SDI トレースをアクティブ化するには、[トレース設定 (Trace Configuration)] ウィンドウで Cisco CTIManager サービスに対して [すべてのトレースをイネーブル化 (Enable All Trace)] をオンにします。[SDL Configuration] ウィンドウにアクセスするには、[Related Links] ドロップダウン リスト ボックスから [**Sdi configuration**] を選択します。「Cisco CTIManager SDL Configuration Trace Filter Settings」の表および「Cisco CTIManager SDL Configuration Trace の特性」の表に記載されている設定が表示されます。

表 45: Cisco CTIManager の SDL 設定に対するトレース フィルタ設定

設定名	説明
各種のポーリングのトレースのイネーブル化。 (Enable miscellaneous polls trace.)	さまざまなポーリングに対するトレースをアクティブ化します。
各種のトレース(データベース信号)のイネーブル化。 (Enable miscellaneous trace (database signals).)	データベースの信号のようなさまざまなトレースをアクティブ化します。
CTIのトレースのイネーブル化。(Enable CTI trace.)	CTIのトレースをアクティブ化します。
ネットワークサービスのデータのトレースのイネーブル化 (Enable network service data trace)	ネットワークサービスのデータのトレースをアクティブ化します。
ネットワークサービスのイベントのトレースのイネーブル化 (Enable network service event trace)	ネットワークサービスのイベントのトレースをアクティブ化します。
ICCP 管理トレースの有効化	ICCP 管理のトレースをアクティブ化します。
デフォルトのトレースのイネーブル化 (Enable Default Trace)	デフォルトのトレースをアクティブ化します。

次の表で、Cisco CTIManager SDL 設定のトレースの特性について説明します。

表 46: Cisco CTIManager SDL の設定に対するトレースの特性

特性	説明
SDL リンク ステートのトレースのイネーブル化。 (Enable SDL link states trace.)	ICCP リンク ステートのトレースをアクティブ化します。
低レベルのSDLのトレースのイネーブル化。 (Enable low-level SDL trace.)	低レベルのSDLのトレースをアクティブ化します。

特性	説明
SDL リンクポーリングトレースを有効にします。	ICCP リンクのポーリングのトレースをアクティブ化します。
SDL リンクメッセージのトレースのイネーブル化。(Enable SDL link messages trace.)	ICCP 未処理メッセージのトレースをアクティブ化します。
信号データダンプトレースを有効にします。	信号データのダンプに対するトレースをアクティブ化します。
関連タグのマッピングのトレースのイネーブル化。(Enable correlation tag mapping trace.)	関連タグのマッピングに対するトレースをアクティブ化します。
SDL プロセスの状態のトレースのイネーブル化。(Enable SDL process states trace.)	SDL プロセス状態のトレースを有効にします。
SDL の pretty プリントのトレースの無効化。(Disable pretty print of SDL trace.)	SDL の pretty プリントに対するトレースを無効化します。pretty プリントでは、後処理を実行しないでトレースファイルにタブとスペースを追加します。
SDL TCP イベントトレースの有効化	SDL TCP イベントのトレースをアクティブ化します。

Cisco Extended Functions のトレース フィールド

次の表では、Cisco Extended Functions のトレースフィールドについて説明します。Cisco Extended Functions サービスは Unified Communications Manager をサポートします。

表 47: Cisco Extended Functions のトレース フィールド

フィールド名	説明
QBEヘルパーCTIのトレースのイネーブル化 (Enable QBE Helper TSP Trace)	テレフォニー サービス プロバイダーのトレースをアクティブ化します。
QBEヘルパーTSPIのトレースのイネーブル化 (Enable QBE Helper TSPI Trace)	QBE ヘルパー TSP インターフェイスのトレースをアクティブ化します。
QRTディクショナリのトレースのイネーブル化 (Enable QRT Dictionary Trace)	Quality report tool サービスディクショナリのトレースをアクティブにします。
DOMヘルパーのトレースのイネーブル化 (Enable DOM Helper Traces)	DOM ヘルパーのトレースをアクティブ化します。
冗長性と変更通知トレースの有効化	データベース変更通知のトレースをアクティブ化します。

フィールド名	説明
QRT レポートハンドラトレースの有効化	品質レポート ツールのレポート ハンドラのトレースをアクティブ化します。
QBE ヘルパー CTI トレースの有効化	QBE ヘルパー CTI のトレースをアクティブ化します。
QRTサービスのトレースのイネーブル化 (Enable QRT Service Trace)	Quality report tool サービス関連トレースをアクティブにします。
QRT DB トレースの有効化	QRT DB アクセスのトレースをアクティブ化します。
テンプレートマップのトレースのイネーブル化 (Enable Template Map Traces)	標準テンプレートマップと multimap トレースをアクティブにします。
QRT イベントハンドラトレースの有効化	品質レポート ツールのイベントハンドラのトレースをアクティブ化します。
QRTリアルタイム情報サーバのトレースのイネーブル化 (Enable QRT Real-Time Information Server Trace)	Quality report tool リアルタイム情報サーバトレースをアクティブにします。

Cisco エクステンション モビリティのトレース フィールド

次の表では、Cisco Extension Mobility のトレースフィールドについて説明します。Cisco Extension Mobility サービスは Unified Communications Manager をサポートします。

表 48: Cisco エクステンション モビリティのトレース フィールド

フィールド名	説明
EMサービスのトレースのイネーブル化 (Enable EM Service Trace)	Cisco エクステンション モビリティ サービスのトレースをアクティブ化します。



ヒント Cisco Extension Mobility アプリケーションサービスのトレースをアクティブ化する場合は、Cisco Cisco Extension Mobility アプリケーションサービスの [トレースの設定 (Trace Configuration)] ウィンドウで [すべてのトレースのイネーブル化 (Enable All Trace)] チェックボックスをオンにします。

Cisco IP Manager Assistant のトレース フィールド

次の表では、Cisco IP Manager Assistant のトレースフィールドについて説明します。Cisco IP Manager Assistant サービスは、Cisco Unified Communications Manager Assistant をサポートしています。

表 49: Cisco IP Manager Assistant のトレース フィールド

フィールド名	説明
IPMAサービスのトレースのイネーブル化 (Enable IPMA Service Trace)	Cisco IP Manager Assistant サービスのトレースをアクティブ化します。
IPMA Managerの設定変更ログのイネーブル化 (Enable IPMA Manager Configuration Change Log)	マネージャとアシスタントの設定に加えた変更のトレースをアクティブにします。
IPMA CTI トレースの有効化	CTI Manager 接続のトレースをアクティブにします。
IPMA CTIセキュリティのトレースのイネーブル化 (Enable IPMA CTI Security Trace)	CTI Managerのセキュアな接続に対するトレースをアクティブ化します。

Cisco IP Voice Media Streaming App のトレース フィールド

ここで説明する内容は、Cisco Unity Connection には適用されません。

次の表では、Cisco IP Voice Media Streaming App トレースのフィールドについて説明します。Cisco IP Voice Media Streaming アプリ サービスは、Unified Communications Manager をサポートします。

表 50: Cisco IP Voice Media Streaming Application のトレース フィールド

フィールド名	説明
サービス初期化のトレースのイネーブル化 (Enable Service Initialization Trace)	初期化情報のトレースをアクティブ化します。
MTPデバイスのトレースのイネーブル化 (Enable MTP Device Trace)	メディア ターミネーション ポイント (MTP) 用に処理されたメッセージをモニタするトレースをアクティブ化します。
デバイスリカバリのトレースのイネーブル化 (Enable Device Recovery Trace)	MTP、会議ブリッジ、MOH に対するデバイスリカバリ情報のトレースをアクティブ化します。
Skinny Stationメッセージのトレースのイネーブル化 (Enable Skinny Station Messages Trace)	Skinny Station Protocol のトレースをアクティブ化します。
WinSockレベル2のトレースのイネーブル化 (Enable WinSock Level 2 Trace)	高レベルで詳細な WinSock 関連情報のトレースをアクティブ化します。
保留音マネージャのトレースのイネーブル化 (Enable Music On Hold Manager Trace)	MOH オーディオ ソース マネージャをモニタするトレースをアクティブ化します。

フィールド名	説明
アナウンサーのトレースのイネーブル化 (Enable Annunciator Trace)	アナウンサーをモニタするトレースをアクティブ化します。
DB設定マネージャのトレースのイネーブル化 (Enable DB Setup Manager Trace)	MTP、会議ブリッジ、MOHに対するデータベース設定や変更をモニタするトレースをアクティブ化します。
会議ブリッジデバイスのトレースの有効化 (Enable Conference Bridge Device Trace)	トレースをアクティブにして、会議ブリッジの処理されたメッセージをモニタします。
デバイスドライバのトレースのイネーブル化 (Enable Device Driver Trace)	デバイスドライバのトレースをアクティブ化します。
WinSockレベル1のトレースのイネーブル化 (Enable WinSock Level 1 Trace)	低レベルで一般的な WinSock 関連情報のトレースをアクティブ化します。
保留音デバイスのトレースのイネーブル化 (Enable Music on Hold Device Trace)	MOH 用に処理されたメッセージをモニタするトレースをアクティブ化します。
TFTPダウンロードのトレースのイネーブル化 (Enable TFTP Downloads Trace)	MOH オーディオ ソース ファイルのダウンロードをモニタするトレースをアクティブ化します。

Cisco TFTP のトレース フィールド

次の表に、Cisco TFTP のトレース フィールドを示します。Cisco TFTP サービスは、Unified Communications Manager をサポートします。

表 51: Cisco TFTP のトレース フィールド

フィールド名	説明
サービスシステムのトレースのイネーブル化 (Enable Service System Trace)	サービスシステムのトレースをアクティブにします。
ビルドファイルのトレースのイネーブル化 (Enable Build File Trace)	ビルドファイルのトレースをアクティブにします。
サーブファイルのトレースのイネーブル化 (Enable Serve File Trace)	サーブファイルのトレースをアクティブにします。

Cisco WebDialer Web サービスのトレース フィールド

次の表では、Cisco Web Dialer Web サービスのトレースフィールドについて説明します。Cisco Web Dialer Web Service は Unified Communications Manager をサポートします。

表 52: Cisco WebDialer Web サービスのトレース フィールド

フィールド名	説明
Web Dialer サーブレットトレースの有効化	Cisco WebDialer Servlet のトレースをアクティブ化します。
リダイレクターサーブレットトレースの有効化	リダイレクターサーブレットのトレースをアクティブにします。

IM and Presence SIP Proxy サービスのトレース フィルタの設定

次の表では、IM and Presence SIP Proxy のトレース フィルタの設定について説明します。

表 53: IM and Presence SIP Proxy サービスのトレース フィルタの設定

パラメータ	説明
Access Log のトレースのイネーブル化 (Enable Access Log Trace)	プロキシ アクセス ログ トレースをイネーブルにします。プロキシが受信した各 SIP メッセージの先頭行がログに記録されます。
Authentication のトレースのイネーブル化 (Enable Authentication Trace)	認証モジュールのトレースをイネーブルにします。
Calendar のトレースのイネーブル化 (Enable CALENDAR Trace)	カレンダー モジュールのトレースをイネーブルにします。
CTI ゲートウェイのトレースのイネーブル化 (Enable CTI Gateway Trace)	CTI ゲートウェイのトレースをイネーブルにします。
Enum のトレースのイネーブル化 (Enable Enum Trace)	Enum モジュールのトレースをイネーブルにします。
Method/Event ルーティングのトレースのイネーブル化 (Enable Method/Event Routing Trace)	メソッド/イベントルーティング モジュールのトレースをイネーブルにします。

パラメータ	説明
Number Expansion のトレースのイネーブル化 (Enable Number Expansion Trace)	Number Expansion モジュールのトレースをイネーブルにします。
Parser のトレースのイネーブル化 (Enable Parser Trace)	sipd の子 SIP パーサーの動作に関するパーサー情報のトレースをイネーブルにします。
Privacy のトレースのイネーブル化 (Enable Privacy Trace)	プライバシー要求に関する PAI、RPID、および Diversion ヘッダーの処理に関する情報のトレースをイネーブルにします。
Registry のトレースのイネーブル化 (Enable Registry Trace)	Registry モジュールのトレースをイネーブルにします。
Routing のトレースのイネーブル化 (Enable Routing Trace)	Routing モジュールのトレースをイネーブルにします。
SIPUA トレースのイネーブル化 (Enable SIPUA Trace)	SIP UA アプリケーション モジュールのトレースをイネーブルにします。
Server のトレースのイネーブル化 (Enable Server Trace)	Server のトレースをイネーブルにします。
SIP メッセージとステート マシンのトレースのイネーブル化 (Enable SIP Message and State Machine Trace)	sipd ごとの SIP マシンの動作に関する情報のトレースをイネーブルにします。
SIP TCP のトレースのイネーブル化 (Enable SIP TCP Trace)	TCP サービスによる SIP メッセージの TCP トランスポートのトレースをイネーブルにします。
SIP TLS のトレースのイネーブル化 (Enable SIP TLS Trace)	TCP サービスによる SIP メッセージの TLS トランスポートのトレースをイネーブルにします。

パラメータ	説明
SIP XMPP IM ゲートウェイ トレースのイネーブル化 (Enable SIP XMPP IM Gateway Trace)	SIP XMPP IM ゲートウェイのトレースをイネーブルにします。
Presence Web Service のトレースのイネーブル化 (Enable Presence Web Service Trace)	Presence Web Service のトレースをイネーブルにします。

IM and Presence トレースフィールドの説明

次の表に、特定のコンポーネントのトレースアクティベーションをサポートするサービスのフィールドの説明を示します。一部のサービスでは、サービスのすべてのトレースをイネーブルにする代わりに、特定のコンポーネントのトレースをアクティブ化できます。この章にないサービスの場合は、[トレース設定 (Trace Configuration)] ウィンドウで、そのサービスに [すべてのトレースをイネーブル化 (Enable All Trace)] が表示されます。

Cisco Access Log のトレースのフィールド

次の表に、Cisco Access Log のトレース フィールドを示します。

表 54: Access Log のトレース フィールド

フィールド名	説明
Access Log のトレースのイネーブル化 (Enable Access Log Trace)	Access Log のトレースを有効にします。

Cisco Authentication のトレースのフィールド

次の表に、Cisco Authentication のトレース フィールドを示します。

表 55: Authentication のトレース フィールド

フィールド名	説明
Authentication のトレースのイネーブル化 (Enable Authentication Trace)	認証トレースを有効にします。

Cisco Calendar のトレースのフィールド

次の表に、Cisco Calendar のトレース フィールドを示します。

表 56: *Calendar* のトレース フィールド

フィールド名	説明
Calendar のトレースのイネーブル化 (Enable CALENDAR Trace)	Calendar のトレースを有効にします。

Cisco CTI ゲートウェイのトレースのフィールド

次の表に、Cisco CTI ゲートウェイのトレース フィールドを示します。

表 57: *CTI* ゲートウェイのトレースのフィールド

フィールド名	説明
CTI ゲートウェイのトレースのイネーブル化 (Enable CTI Gateway Trace)	CTI ゲートウェイのトレースを有効にします。

Cisco Database Layer Monitor のトレースのフィールド

次の表に、Cisco Database Layer Monitor のトレース フィールドを示します。

表 58: *Cisco Database Layer Monitor* のトレースのフィールド

フィールド名	説明
DB ライブラリ トレースのイネーブル化 (Enable DB Library Trace)	C++アプリケーションのデータベースライブラリのトレースをイネーブルにします。
サービスのトレースのイネーブル化 (Enable Service Trace)	サービストレースをオンにします。
DB変更通知のトレースのイネーブル化 (Enable DB Change Notification Trace)	C++アプリケーションのデータベース変更通知トレースを有効にします。
単体試験のトレースのイネーブル化 (Enable Unit Test Trace)	オンにしません。デバッグ目的でシスコのエンジニアが使用します。

Cisco Enum のトレース フィールド

次の表に、Cisco Enum のトレース フィールドを示します。

表 59: *Enum* のトレース フィールド

フィールド名	説明
Enum のトレースのイネーブル化 (Enable Enum Trace)	Enum のトレースをアクティブ化します。

Cisco Method/Event のトレース フィールド

次の表では、Cisco Method/Event トレースフィールドについて説明します。

表 60: メソッド/イベントトレースのフィールド

フィールド名	説明
Method/Event のトレースのイネーブル化 (Enable Method/Event Trace)	Method/Event のトレースをイネーブルにします。

Cisco Number Expansion のトレース フィールド

次の表に、Cisco Number Expansion のトレース フィールドを示します。

表 61: *Number Expansion* のトレース フィールド

フィールド名	説明
Number Expansion のトレースのイネーブル化 (Enable Number Expansion Trace)	Number Expansion のトレースを有効にします。

Cisco Parser のトレース フィールド

次の表に、Cisco Parser のトレース フィールドを示します。

表 62: *Parser* のトレース フィールド

フィールド名	説明
Parser のトレースのイネーブル化 (Enable Parser Trace)	Parser のトレースを有効にします。

Cisco Privacy のトレースのフィールド

次の表に、Cisco Privacy のトレース フィールドを示します。

表 63: *Privacy* のトレース フィールド

フィールド名	説明
Privacy のトレースのイネーブル化 (Enable Privacy Trace)	Privacy のトレースをアクティブ化します。

Cisco Proxy のトレース フィールド

次の表に、Cisco Proxy のトレース フィールドを示します。

表 64: Proxy のトレース フィールド

フィールド名	説明
代理権限	Proxy のトレースをアクティブ化します。

Cisco RIS Data Collector のトレースのフィールド

次の表に、Cisco RIS Data Collector のトレース フィールドを示します。

表 65: Cisco RIS Data Collector のトレースのフィールド

フィールド名	説明
RISDC のトレースのイネーブル化 (Enable RISDC Trace)	RIS データ コレクタ サービス (RIS) の RISDC スレッドのトレースをアクティブ化します。
システムアクセスのトレースのイネーブル化 (Enable System Access Trace)	RIS データ コレクタのシステム アクセス ライブラリのトレースをアクティブ化します。
リンクサービスのトレースのイネーブル化 (Enable Link Services Trace)	RIS データ コレクタのリンク サービス ライブラリのトレースをアクティブ化します。
RISDCアクセスのトレースのイネーブル化 (Enable RISDC Access Trace)	RIS データ コレクタの RISDC アクセス ライブラリのトレースをアクティブ化します。
RISDB のトレースのイネーブル化 (Enable RISDB Trace)	RIS データ コレクタの RISDB ライブラリのトレースを有効にします。
PI のトレースのイネーブル化 (Enable PI Trace)	RIS データ コレクタの PI ライブラリのトレースを有効にします。
XML のトレースのイネーブル化 (Enable XML Trace)	RIS データ コレクタ サービスの入出力 XML メッセージのトレースを有効にします。
Perfmon ロガーのトレースのイネーブル化 (Enable Perfmon Logger Trace)	RIS データ コレクタの perfmon データ ロギングをトラブルシューティングするためのトレースを有効にします。ログファイル、記録されたカウンタの総数、アプリケーションおよびシステムカウンタとインスタンスの名前、プロセスとスレッドの CPU パーセンテージの計算、ログファイルのロールオーバーと削除の発生をトレースするために使用します。

Cisco Registry のトレースのフィールド

次の表に、Cisco Registry のトレース フィールドを示します。

表 66: Registry のトレース フィールド

フィールド名	説明
Registry のトレースのイネーブル化 (Enable Registry Trace)	Registry のトレースを有効にします。

Cisco Routing のトレースのフィールド

次の表に、Cisco Routing のトレース フィールドを示します。

表 67: Routing のトレース フィールド

フィールド名	説明
Routing のトレースのイネーブル化 (Enable Routing Trace)	ルーティング トレースを有効にします。

Cisco Server のトレースのフィールド

次の表に、Cisco Server のトレース フィールドを示します。

表 68: Server のトレース フィールド

フィールド名	説明
Server のトレースのイネーブル化 (Enable Server Trace)	Server のトレースをアクティブ化します。

Cisco SIP Message と State Machine のトレースのフィールド

次の表に、Cisco SIP Message と State Machine のトレース フィールドを示します。

表 69: SIP Message と State Machine のトレース フィールド

フィールド名	説明
SIP メッセージとステート マシンのトレースのイネーブル化 (Enable SIP Message and State Machine Trace)	SIP メッセージとステート マシンのトレースを有効にします。

Cisco SIP TCP のトレース フィールド

次の表に、Cisco SIP TCP のトレース フィールドを示します。

表 70: SIP TCP のトレース フィールド

フィールド名	説明
SIP TCP のトレースのイネーブル化 (Enable SIP TCP Trace)	SIP TCP のトレースを有効にします。

Cisco SIP TLS のトレースのフィールド

次の表に、Cisco SIP TLS のトレース フィールドを示します。

表 71: SIP TLS のトレース フィールド

フィールド名	説明
SIP TLS のトレースのイネーブル化 (Enable SIP TLS Trace)	SIP TLS のトレースを有効にします。

Cisco Web Service のトレースのフィールド

次の表に、Cisco Web Service のトレース フィールドを示します。

表 72: Web Service のトレース フィールド

フィールド名	説明
Presence Web Service のトレースのイネーブル化 (Enable Presence Web Service Trace)	Presence Web Service のトレースを有効にします。

Trace Output Settings

次の表に、トレース ログ ファイルの説明を示します。



注意 [トレース設定 (Trace Configuration)] ウィンドウで [最大ファイル数 (Maximum No. of Files)] または [最大ファイル サイズ (Maximum File Size)] を変更すると、サービスが実行中の場合は現在のファイル以外のすべてのサービスログファイルが削除されます。サービスがアクティブ化されていない場合は、サービスをアクティブ化したときにただちにファイルが削除されます。ログ ファイルの記録を保持する必要がある場合は、[最大ファイル数 (Maximum No. of Files)] または [最大ファイル サイズ (Maximum File Size)] の設定を変更する前に、サービスログファイルをダウンロードして別のサーバに保存してください。そのためには、Unity RTMT の Trace and Log Central を使用します。

表 73: Trace Output Settings

フィールド	説明
最大ファイル数 (Maximum number of files)	指定したサービスのトレースファイルの総数を指定します。 Cisco Unified Serviceability では、ファイルを識別するために、cus299.txt のようにファイル名にシーケンス番号が自動的に追加されます。シーケンス中の最後のファイルが一杯になると、最初のファイルのトレースデータが上書きされます。デフォルトはサービスによって異なります。
最大ファイルサイズ(MB) (Maximum file size (MB))	トレースファイルの最大サイズ (MB 単位) を指定します。デフォルトはサービスによって異なります。

トレース設定のトラブルシューティング

トラブルシューティング トレース設定ウィンドウ

[トラブルシューティング トレース設定 (Troubleshooting Trace Settings)] ウィンドウでは、事前に設定されたトラブルシューティング トレース設定を行う Serviceability GUI のサービスを選択できます。このウィンドウでは、クラスタ内の異なる ノードに対してサービスを選択できます。これにより、選択したすべてのサービスのトレース設定の変更が行われます。1台のノードの特定のアクティブなサービスの選択、そのノードのすべてのアクティブなサービスの選択、クラスタ内のすべてのノードの特定のアクティブなサービスの選択、クラスタ内のすべてのノードのすべてのアクティブなサービスの選択が可能です。このウィンドウでは、非アクティブなサーバの横に [N/A] と表示されます。



- (注) IM and Presence の場合、IM and Presence 機能またはネットワーク サービスの事前に決定されたトラブルシューティング トレース設定には、SDI および Log4j トレースの設定があります。トラブルシューティング トレース設定が適用される前に、元のトレース設定がバックアップされます。トラブルシューティング トレース設定をリセットすると、元のトレース設定が復元されます。

トラブルシューティング トレース設定をサービスに適用した後で [トラブルシューティング トレース設定 (Troubleshooting Trace Settings)] ウィンドウを開くと、トラブルシューティング用に設定したサービスがチェック付きで表示されます。[トラブルシューティング トレース設定 (Troubleshooting Trace Settings)] ウィンドウでは、トレース設定を元の設定にリセットできません。

トラブルシューティング トレース設定をサービスに適用すると、トラブルシューティング トレースがそのサービスに設定されたことを示すメッセージが [トレース設定 (Trace Configuration)] ウィンドウに表示されます。サービスの設定をリセットする場合は、[関連リンク (Related Links)] リスト ボックスから、[トラブルシューティング トレース設定 (Troubleshooting Trace Settings)] オプションを選択できます。指定したサービスの [トレース設定 (Trace Configuration)] ウィンドウでは、すべての設定が読み取り専用として表示されません。ただし、最大ファイル数など、トレース出力設定の一部のパラメータを除きます。

トラブルシューティング トレース設定

始める前に

トレース設定のセットアップタスクを確認し、トレースパラメータを設定します。

手順

ステップ 1 [トレース (Trace)] > [トラブルシューティング トレース設定 (Troubleshooting Trace Settings)] を選択します。

ステップ 2 [サーバ (Server)] リスト ボックスから、トレース設定をトラブルシューティングするサーバを選択します。

ステップ 3 [移動 (Go)] を選択します。

サービスの一覧が表示されます。アクティブ化されていないサービスは、[該当なし (N/A)] と表示されます。

ステップ 4 次のいずれかの操作を実行します。

a) [サーバ (Server)] リスト ボックスで選択したノードの特定のサービスをモニタするには、[サービス (Services)] ペインでそのサービスをオンにします。

たとえば、[データベースおよび管理サービス (Database and Admin Services)]、[パフォーマンスおよびモニタリングサービス (Performance and Monitoring Services)]、[バックアップおよび復元サービス (Backup and Restore Services)] ペインなどがあります。

この作業は、[サーバ (Server)] リスト ボックスで選択したノードのみに影響します。

b) [サーバ (Server)] リスト ボックスで選択したノードのすべてのサービスをモニタするには、[すべてのサービスをチェック (Check All Services)] をオンにします。

c) Cisco Unified Communications Manager および IM and Presence クラスタのみ：クラスタ内のすべてのノードで特定のサービスをモニタするには、[すべてのノードで選択されたサービスをチェック (Check Selected Services on All Nodes)] をチェックします。

この設定は、クラスタ内のサービスがアクティブなすべてのノードに適用されます。

d) Unified Communications Manager and IM and Presence クラスタのみ：クラスタのすべてのサービスをモニタするには、**すべてのノードのすべてのサービスをチェックする**をオンにします。

ステップ 5 [保存] を選択します。

ステップ 6 元のトレース設定に戻すには、次のいずれかのボタンをクリックします。

- a) [トラブルシューティングトレースをリセット (Reset Troubleshooting Traces)]: [サーバ (Server)]リストボックスで選択したノードで元のトレース設定を復元します。また、選択可能なアイコンも表示されます。
- b) Cisco Unified Communications Manager および IM and Presence クラスタのみ: [すべてのノードでトラブルシューティングトレースをリセット (Reset Troubleshooting Traces On All Nodes)]: クラスタ内のすべてのノードでサービスの元のトレース設定を復元します。

[トラブルシューティングトレースをリセット (Reset Troubleshooting Traces)] ボタンは、1 つ以上のサービスのトラブルシューティング トレースを設定してある場合にのみ表示されます。

(注) トラブルシューティングトレースを長時間イネーブルのままにすると、トレースファイルのサイズが大きくなり、サービスのパフォーマンスに影響が生じるおそれがあります。

[リセット (Reset)] ボタンをクリックすると、ウィンドウが更新され、サービスのチェックボックスがオフになります。



第 18 章

使用状況レコードの表示

- [使用状況レコードの概要 \(303 ページ\)](#)
- [使用状況レポートのタスク \(304 ページ\)](#)

使用状況レコードの概要

Cisco Unified Communications Manager が提供するレコードを使用して、設定済みの項目がシステム内でどのように使用されているのかを確認することができます。設定済みの項目には、デバイスだけでなく、デバイスプール、日時グループ、ルートプランなどのシステムレベルの設定も含まれます。

依存関係レコード

依存関係レコードは、次の目的で使用します。

- システムレベルの設定（サーバ、デバイスプール、日時グループなど）に関する情報を調べる。
- 他のレコードを使用しているデータベース内のレコードを確認する。たとえば、特定のコーリング検索スペースを使用しているデバイス（CTIルートポイントや電話機など）を確認できます。
- レコードを削除する前に、レコード間の依存関係を明らかにする。たとえば、パーティションを削除する前に、依存関係レコードを使用して、そのパーティションにどのコーリング検索スペース（CSS）とデバイスが関連付けられているかを確認します。こうすることで、その依存関係を削除するように設定を再構成できます。

ルートプランレポート

ルートプランレポートでは、システム内で設定されている番号、ルート、パターンの一部またはすべてを確認できます。レポートを生成する際は、レポートの [パターン/電話番号 (Pattern/Directory Number)] 列、[パーティション (Partition)] 列、または [ルート詳細 (Route

Detail)]列のエントリをクリックすることで、該当する項目の設定ウィンドウにアクセスできます。

さらに、ルートプランレポートを使用してレポートデータを .CSV ファイルに保存し、そのファイルを他のアプリケーションにインポートすることもできます。保存される .CSV ファイルには、ウェブ ページより詳細な情報（電話機の電話番号、ルートパターン、パターン使用法、デバイス名、デバイスの説明など）が含まれます。

Cisco Unified Communications Manager は、内部コールのルーティングにも、外部公衆電話交換網（PSTN）コールのルーティングにもルートプランを使用します。ネットワーク内には複数のレコードがある可能性があるため、Cisco Unified Communications Manager Administration では特定の基準に基づいて特定のルートプランレコードを検索できるようになっています。

使用状況レポートのタスク

手順

	コマンドまたはアクション	目的
ステップ 1	<p>ルートプランレコードを表示し、これらのレコードを使用して未割り当ての電話番号を管理するには、次の手順を参照してください。</p> <ul style="list-style-type: none"> • ルートプランレコードの表示 (305 ページ) • ルートプランレコードの保存 (306 ページ) • 未割り当ての電話番号の削除 (306 ページ) • 未割り当ての電話番号の更新 (307 ページ) 	<p>特定のルートプランレコードを検索し、レコードを CSV ファイルに保存し、未割り当ての電話番号を管理するには、これらの手順を使用してください。</p>
ステップ 2	<p>依存関係レコードを使用するには、次の手順を参照してください。</p> <ul style="list-style-type: none"> • 依存関係レコードの表示 (309 ページ) 	<p>システムレベルの設定に関する情報を見つけ、データベース内のレコード間の依存関係を表示するには、これらの手順を使用してください。</p>

ルート プラン レポートのタスク フロー

手順

	コマンドまたはアクション	目的
ステップ 1	ルートプランレコードの表示 (305 ページ)。	ルート プラン レコードを表示し、カスタマイズされたルート プラン レポートを生成します。
ステップ 2	ルートプランレコードの保存 (306 ページ)。	.csv ファイル形式でルート プラン レポートを表示します。
ステップ 3	未割り当ての電話番号の削除 (306 ページ)。	ルート プラン レポートから未割り当ての電話番号を削除します。
ステップ 4	未割り当ての電話番号の更新 (307 ページ)。	ルート プラン レポートから未割り当ての電話番号の設定を更新します。

ルート プラン レコードの表示

ここでは、ルート プラン レコードを表示する方法について説明します。ネットワーク内に複数のレコードがある可能性があるため、[Cisco Unified Communications Managerの管理 (Cisco Unified Communications Manager Administration)] では、特定の基準に基づいて特定のルート プラン レコードを検索できます。カスタマイズされたルート プラン レポートを生成するには、次の手順を実行します。

手順

ステップ 1 [コール ルーティング (Call Routing)] > [ルート プラン レポート (Route Plan Report)] の順に選択します。

ステップ 2 データベースのすべてのレコードを検索するには、ダイアログボックスが空であることを確認して、ステップ 3 に進みます。

レコードをフィルタまたは検索するには、次の手順を実行します。

- 最初のドロップダウン リスト ボックスで、検索パラメータを選択します。
- 2 番目のドロップダウン リスト ボックスで、検索パターンを選択します。
- 必要に応じて、適切な検索テキストを指定します。

ステップ 3 [検索 (Find)] をクリックします。

すべてのレコードまたは一致するレコードが表示されます。1 ページあたりの項目の表示件数を変更するには、[ページあたりの行数 (Rows per Page)] ドロップダウン リスト ボックスで別の値を選択します。

ステップ 4 表示されるレコードのリストで、表示するレコードのリンクをクリックします。

選択した項目がウィンドウに表示されます。

ルート プラン レコードの保存

このセクションでは、.csv ファイルでルート プラン レポートを表示する方法について説明します。

手順

ステップ 1 [コール ルーティング (Call Routing)] > [ルート プラン レポート (Route Plan Report)] の順に選択します。

ステップ 2 [ルート プラン レポート (Route Plan Report)] ウィンドウの [関連リンク (Related Links)] ドロップダウンリストから [ファイルで表示 (View In File)] を選択し、[移動 (Go)] をクリックします。

表示されたダイアログボックスで、ファイルを保存するか、別のアプリケーションにファイルをインポートすることができます。

ステップ 3 [保存 (Save)] をクリックします。

別のウィンドウが表示され、任意の場所にこのファイルを保存できます。

(注) 別のファイル名での保存も可能ですが、ファイル名には .CSV 拡張子を含める必要があります。

ステップ 4 ファイルを保存する場所を選択し、[保存 (Save)] をクリックします。この操作により、指定した場所にファイルが保存されます。

ステップ 5 保存した .CSV ファイルを探し、アイコンをダブルクリックして表示します。

未割り当ての電話番号の削除

このセクションでは、ルート プラン レポートから未割り当ての電話番号を削除する方法について説明します。電話番号は、Cisco Unified Communications Manager Administration の [電話番号の設定 (Directory Number Configuration)] ウィンドウで設定または削除します。電話番号がデバイスから削除されたり、電話機が削除されたりしても、電話番号はそのまま Cisco Unified Communications Manager データベース内に残ります。データベースから電話番号を削除するには、[ルート プラン レポート (Route Plan Report)] ウィンドウを使用します。

手順

ステップ 1 [コール ルーティング (Call Routing)] > [ルート プラン レポート (Route Plan Report)] を選択します。

ステップ 2 [ルートプランレポート (Route Plan Report)] ウィンドウで、3つのドロップダウンリストを使用して、すべての未割り当て DN を列挙するルートプランレポートを指定します。

ステップ 3 電話番号を削除する3つの方法があります。

- a) 削除する電話番号をクリックします。[電話番号の設定 (Directory Number Configuration)] ウィンドウが表示されたら、[削除 (Delete)] をクリックします。
- b) 削除する電話番号の横にあるチェックボックスをオンにします。[選択項目の削除] をクリックします。
- c) 見つかった未割り当ての電話番号をすべて削除するには、[見つかった項目をすべて削除 (Delete All Found Items)] をクリックします。

電話番号を削除するかどうかを確認する警告メッセージが表示されます。

ステップ 4 電話番号を削除する場合は、[OK] をクリックします。削除要求をキャンセルする場合は、[キャンセル (Cancel)] をクリックします。

未割り当ての電話番号の更新

この項では、ルートプランレポートから未割り当ての電話番号の設定を更新する方法について説明します。電話番号は、Cisco Unified Communications Manager Administration の [電話番号の設定 (Directory Number Configuration)] ウィンドウで設定または削除します。デバイスから電話番号が削除されても、電話番号は Cisco Unified Communications Manager データベースに残っています。電話番号の設定を更新するには、[ルートプランレポート (Route Plan Report)] ウィンドウを使用します。

手順

ステップ 1 [コールルーティング (Call Routing)] > [ルートプランレポート (Route Plan Report)] を選択します。

ステップ 2 [ルートプランレポート (Route Plan Report)] ウィンドウで、3つのドロップダウンリストを使用して、未割り当ての電話番号をすべてリストするルートプランレポートを指定します。

ステップ 3 更新する電話番号をクリックします。

(注) 電話番号およびパーティションを除く、電話番号のすべての設定を更新できます。

ステップ 4 コーリングサーチスペースや転送オプションなどの必要な更新を行います。

ステップ 5 [保存 (Save)] をクリックします。

[電話番号の設定 (Directory Number Configuration)] ウィンドウが再度表示され、電話番号フィールドが空になります。

依存関係レコードタスクフロー

手順

	コマンドまたはアクション	目的
ステップ 1	依存関係レコードの設定 (308 ページ)。	この手順を使用して、依存関係レコードを有効または無効にします。この手順は、通常よりも低い優先順位で実行され、ダイヤルプランの規模と複雑さ、CPU 速度、およびその他のアプリケーションの CPU 要件によっては完了までに時間がかかることがあります。
ステップ 2	依存関係レコードの表示 (309 ページ)。	依存関係レコードを有効にしたら、インターフェイスの設定ウィンドウからそれらのレコードにアクセスできるようになります。

依存関係レコードの設定

依存レコードを使用して、Cisco Unified Communications Manager データベース内のレコード間の関係を表示します。たとえば、パーティションを削除する前に、依存関係レコードを使用して、そのパーティションにどのコーリング検索スペース (CSS) とデバイスが関連付けられているかを確認します。



注意 依存関係レコードを使用すると、CPU 使用率が高くなります。この手順は、標準以下の優先順位で動作し、ダイヤルプランのサイズと複雑さ、CPU 速度、および他のアプリケーションの CPU 要件によっては、完了までに時間がかかる場合があります。

依存関係レコードを有効にしたために、システムで CPU 使用率の問題が発生している場合は、依存関係レコードを無効にすることができます。

手順

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

ステップ 2 [CCMAdmin パラメータ (CCMAdmin Parameters)] セクションにスクロールし、[依存関係レコードの有効化 (Enable Dependency Records)] ドロップダウンリストで、次のオプションのいずれかを選択します。

- [True] : 依存関係レコードを有効にします。
- [False] : 依存関係レコードを無効にします。

選択したオプションに基づいて、依存関係レコードを有効または無効にした結果に関するメッセージを含むダイアログボックスが表示されます。このダイアログボックスで、[OK]をクリックする前に、メッセージをお読みください。

ステップ 3 [OK] をクリックします。

ステップ 4 [保存 (Save)] をクリックします。

変更を確認する「更新に成功しました (Update Successful) 」メッセージが表示されます。

依存関係レコードの表示

依存関係レコードを有効にすると、インターフェイスの設定ウィンドウからそれらにアクセスできます。

始める前に

[依存関係レコードの設定 \(308 ページ\)](#)

手順

ステップ 1 Cisco Unified CM の管理から、表示するレコードの設定ウィンドウに移動します。

例：

デバイス プールの依存関係レコードを表示するには、[システム (System)] > [デバイス プール (Device Pool)] を選択します。

(注) [デバイスのデフォルト (Device Defaults)] ウィンドウと [エンタープライズパラメータ設定 (Enterprise Parameters Configuration)] ウィンドウで依存関係レコードを表示することはできません。

ステップ 2 [検索 (Find)] をクリックします。

ステップ 3 レコードのいずれかをクリックします。
設定ウィンドウが表示されます。

ステップ 4 [関連リンク (Related Links)] リストボックスで、[依存関係レコード (Dependency Records)] を選択し、[移動 (Go)] をクリックします。

(注) 依存関係レコードを有効にしていない場合は、[依存関係レコード要約 (Dependency Records Summary)] ウィンドウに、レコードに関する情報ではなくメッセージが表示されます。

[依存関係レコード要約 (Dependency Records Summary)] ウィンドウには、データベース内の他のレコードによって使用されるレコードが表示されます。

ステップ 5 このウィンドウで、次の依存関係レコード ボタンのいずれかを選択します。

- [更新 (Refresh)] : 最新の情報でウィンドウを更新します。

- [閉じる (Close)] : [依存関係レコード (Dependency Records)] リンクをクリックした設定ウィンドウに戻らずにウィンドウを閉じます。
 - [閉じて戻る (Close and Go Back)] : ウィンドウを閉じて、[依存関係レコード (Dependency Records)] リンクをクリックした設定ウィンドウに戻ります。
-



第 19 章

エンタープライズパラメータの管理

- ・ [エンタープライズパラメータの概要 \(311 ページ\)](#)

エンタープライズパラメータの概要

エンタープライズパラメータは、クラスタ全体ですべてのデバイスやサービスに適用されるデフォルト設定を提供します。たとえば、システムではエンタープライズパラメータを使用してデバイスのデフォルトの初期値を設定します。

ユーザはエンタープライズパラメータを追加または削除できませんが、既存のエンタープライズパラメータを更新することはできます。エンタープライズパラメータの設定ウィンドウには、カテゴリ（CCMAdmin パラメータ、CCMUser パラメータ、CDR パラメータなど）ごとにエンタープライズパラメータが一覧表示されます。

エンタープライズパラメータの詳細な説明は、[エンタープライズパラメータ設定（Enterprise Parameters Configuration）] ウィンドウで確認できます。



注意 エンタープライズパラメータの多くは、変更する必要がありません。変更しようとしている機能を完全に理解している場合、または Cisco Technical Assistance Center (TAC) から変更を指示された場合を除き、エンタープライズパラメータを変更しないでください。

エンタープライズパラメータ情報の表示

[エンタープライズパラメータ設定（Enterprise Parameter Configuration）] ウィンドウで、埋め込まれたコンテンツを通してエンタープライズパラメータに関する情報にアクセスします。

手順

- ステップ 1** Cisco Unified CM Administration から、[システム（System）] > [エンタープライズパラメータ（Enterprise Parameters）] を選択します。
- ステップ 2** 次のいずれかの作業を実行します。

- 特定のエンタープライズパラメータの説明を表示するには、パラメータ名をクリックします。
- エンタープライズパラメータの説明をすべて表示するには、[?] をクリックします。

エンタープライズパラメータの更新

次の手順を使用して、[エンタープライズパラメータ設定 (Enterprise Parameter Configuration)] ウィンドウを開き、システム レベル設定を構成します。



注意 エンタープライズパラメータの多くは、変更する必要がありません。変更しようとしている機能を完全に理解している場合、または Cisco Technical Assistance Center (TAC) から変更を指示された場合を除き、エンタープライズパラメータを変更しないでください。

手順

- ステップ 1** Cisco Unified CM Administration から、[システム (System)] > [エンタープライズパラメータ (Enterprise Parameters)] を選択します。
- ステップ 2** 変更するエンタープライズパラメータに必要な値を選択します。
- ステップ 3** [保存 (Save)] をクリックします。

次のタスク

[デバイスへの設定の適用 \(312 ページ\)](#)

デバイスへの設定の適用

次の手順を使用して、構成した設定でクラスタ内のすべての影響を受けるデバイスを更新します。

始める前に

[エンタープライズパラメータの更新 \(312 ページ\)](#)

手順

- ステップ 1** Cisco Unified CM Administration から、[システム (System)] > [エンタープライズパラメータ (Enterprise Parameters)] を選択します。
- ステップ 2** 変更を確認してから、[保存 (Save)] をクリックします。

ステップ3 次のいずれかのオプションを選択します。

- システムでリポートするデバイスを判断するには、[設定の適用 (Apply Config)] をクリックします。リポートする必要がないデバイスもあります。進行中のコールはドロップされる可能性があります。接続されたコールは、デバイスプールにSIPトランクが含まれていない限り、保持されます。
- クラスタ内のすべてのデバイスをリポートするには、[リセット (Reset)] をクリックします。この手順はオフピーク時間帯に実行することをお勧めします。

ステップ4 確認ダイアログを読んでから、[OK] をクリックします。

デフォルト エンタープライズ パラメータの復元

エンタープライズ パラメータをデフォルト設定にリセットする場合は、次の手順を使用します。一部のエンタープライズパラメータには、設定ウィンドウの列に示すように、推奨値が含まれています。この手順では、これらの値をデフォルト設定として使用します。

手順

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

ステップ2 [デフォルトに設定 (Set to Default)] をクリックします。

ステップ3 確認プロンプトを読み、[OK] をクリックします。



第 20 章

サーバの管理

- [サーバの管理の概要 \(315 ページ\)](#)
- [サーバの削除 \(315 ページ\)](#)
- [インストール前のクラスタへのノードの追加 \(319 ページ\)](#)
- [プレゼンス サーバのステータスの表示 \(320 ページ\)](#)
- [ポートの設定 \(321 ページ\)](#)
- [ホスト名の設定 \(323 ページ\)](#)
- [Kerneldump ユーティリティ \(324 ページ\)](#)

サーバの管理の概要

この章では、Cisco Unified Communications Manager ノードのプロパティを管理する方法、プレゼンス サーバのステータスを表示する方法、および Unified Communications Manager サーバのホスト名を設定する方法を説明します。

サーバの削除

ここでは、Cisco Unified Communications Manager データベースからサーバを削除する方法と、削除されたサーバを Cisco Unified Communications Manager クラスタに追加する方法について説明します。

Cisco Unified Communications Manager Administration では、クラスタの最初のノードを削除することはできませんが、後続のノードは削除できます。[サーバの検索/一覧表示 (Find and List Servers)] ウィンドウで後続のノードを削除する前に、Cisco Unified CM Administration に次のメッセージが表示されます。「1つ以上のサーバを完全に削除しようとしています。この操作は元に戻せません。続行しますか?」というメッセージが表示されます。[OK] をクリックすると、サーバは Cisco Unified CM データベースから削除され、使用できなくなります。



ヒント [サーバの設定 (Server Configuration)] ウィンドウからサーバを削除しようとするすると、前のパラグラフのメッセージが表示されます。[OK]をクリックすると、サーバは Cisco UnifiedCM データベースから削除され、使用できなくなります。

サーバを削除する前に、次の情報を考慮してください。

- Cisco Unified Communications Manager Administrationでは、クラスタ内の最初のノードを削除することはできませんが、後続のノードは削除できます。
- シスコでは、特にノードに電話機などのデバイスが登録されている場合に、そのノードで実行されている Cisco Unified Communications Manager のノードを削除しないことを推奨しています。
- 後続ノードの依存関係レコードは存在しますが、このレコードではノードを削除することはできません。
- 削除するノードの Cisco Unified Communications Manager にコールパーク番号が設定されている場合は、削除できません。ノードを削除するには、Cisco Unified CM の管理でコールパーク番号を削除する必要があります。
- Cisco Unified Communications Manager Administration の設定フィールドに、削除する予定のサーバの IP アドレスまたはホスト名が含まれている場合は、サーバを削除する前に設定を更新します。このタスクを実行しない場合、設定に依存する機能は、サーバを削除した後に機能しない可能性があります。たとえば、サービスパラメータ、エンタープライズパラメータ、サービス URL、ディレクトリ URL、IP phone サービスなどの IP アドレスまたはホスト名を入力する場合は、サーバを削除する前にこの設定を更新します。
- たとえば、Cisco Unity、Cisco Unity Connection などのアプリケーション GUI に、削除する予定のサーバの IP アドレスまたはホスト名が含まれている場合は、サーバを削除する前に、対応する gui の設定を更新します。このタスクを実行しない場合、設定に依存する機能は、サーバを削除した後に機能しない可能性があります。
- サーバを削除すると、システムによって MOH サーバなどの一部のデバイスが自動的に削除されることがあります。
- ノードを削除する前に、後続のノードでアクティブになっているサービスを非アクティブにすることを推奨します。このタスクを実行すると、ノードを削除した後でサービスが動作することが保証されます。
- サーバの構成に加えた変更は、Cisco Unified Communications Manager を再起動するまで有効になりません。Cisco CallManager サービスの再起動については、『Cisco Unified Serviceability Administration Guide』を参照してください。
- データベースファイルが正しく更新されるようにするには、サーバ、プレゼンス、またはアプリケーションサーバを削除した後に、クラスタを再起動する必要があります。
- ノードを削除した後、Cisco ユニファイドレポートにアクセスして、Cisco Unified Communications Manager クラスタからノードが削除されたことを確認します。さらに、Cisco

Unified Reporting、RTMT、または CLI にアクセスして既存のノード間でデータベースレプリケーションが行われていることを確認し、必要であれば、CLI を使用してノード間のデータベースレプリケーションを修復してください。



(注) サブスクリバードがクラスタから削除されても、その証明書はパブリッシャーおよび他のノードに引き続き存在します。管理者は手動で削除する必要があります。

- 個々のクラスタメンバーの信頼ストアから削除されたサブスクリバードの証明書。
- 削除されたサブスクリバードの信頼ストアから他の各クラスタメンバーの証明書。

クラスタからの Unified Communications Manager ノードの削除

クラスタから Cisco Unified Communications Manager ノードを削除するには、次の手順を実行します。

手順

- ステップ 1** Cisco Unified CM Administration から、[システム (System)] > [サーバ (Server)] を選択します。
- ステップ 2** [検索 (Find)] をクリックして、削除するノードを選択します。
- ステップ 3** [削除 (Delete)] をクリックします。
- ステップ 4** このアクションを取り消せないことを示す警告ダイアログボックスが表示されたら、[OK] をクリックします。
- ステップ 5** 割り当てを解除したノードのホスト VM をシャットダウンします。

クラスタからの IM and Presence ノードの削除

プレゼンス冗長グループおよびクラスタから IM and Presence Service ノードを安全に削除する必要がある場合は、この手順に従います。



注意 ノードを削除すると、そのプレゼンス冗長グループの残りのノードで、ユーザに対するサービスが中断されます。この手順は必ず、メンテナンス期間中に実行してください。

手順

-
- ステップ 1** [Cisco Unified CM の管理 (Cisco Unified CM Administration)] > [システム (System)] > [プレゼンス冗長グループ (Presence Redundancy Groups)] ページで、高可用性が有効な場合は無効にします。
- ステップ 2** [Cisco Unified CM の管理 (Cisco Unified CM Administration)] > [ユーザ管理 (User Management)] > [プレゼンスユーザの割り当て (Assign Presence Users)] ページで、削除するノードからすべてのユーザの割り当てを解除するか、移動します。
- ステップ 3** プレゼンス冗長グループからノードを削除するには、プレゼンス冗長グループの [プレゼンス冗長グループの設定 (Presence Redundancy Group Configuration)] ページの [プレゼンスサーバ (Presence Server)] ドロップダウンリストから、[未選択 (Not-Selected)] を選択します。ノードの割り当て解除の結果としてプレゼンス冗長グループ内のサービスが再起動されることを示す警告ダイアログボックスが表示されたら、[OK] を選択します。
- (注) プレゼンス冗長グループから直接パブリッシャノードを削除することはできません。パブリッシャノードを削除するには、まずパブリッシャノードからユーザの割り当てを解除し、プレゼンス冗長グループを完全に削除します。
- ただし、削除された IM and Presence ノードをクラスタに再び追加することができます。削除されたノードを追加する方法の詳細に [削除したサーバをクラスタに戻す \(318 ページ\)](#) については、を参照してください。このシナリオでは、Cisco DefaultCUPSubcluster CM Administration コンソールの [System > server] 画面で、削除されたパブリッシャノードがサーバに再び追加されると、が自動的に作成されます。
- ステップ 4** Cisco Unified CM Administration で、[システム (System)] > [サーバ (Server)] から未割り当てのノードを削除します。この操作は取り消せないことを示す警告ダイアログボックスが表示されたら、[OK] をクリックします。
- ステップ 5** 割り当てを解除したノードのホスト VM またはサーバをシャットダウンします。
- ステップ 6** すべてのノードの **Cisco XCP Router** を再起動します。
-

削除したサーバをクラスタに戻す

Unified Communications Manager Administration から後続のノード (サブスクライバ) を削除してそれをクラスタに戻す場合に、次の手順を実行します。

手順

-
- ステップ 1** Cisco Unified Communications Manager Administration で、[システム (System)] > [サーバ (Server)] を選択してサーバを追加します。

ステップ2 後続のノードを Cisco Unified Communications Manager Administration に追加したら、シスコが提供しているソフトウェアキットに付属しているご使用のバージョン用のディスクを使用して、サーバ上でインストールを実行します。

ヒント インストールするバージョンが、パブリッシャノード上で動作しているバージョンと一致することを確認します。パブリッシャ上で実行されているバージョンがインストールファイルと一致しない場合は、インストールプロセス中に[インストール中にアップグレード (Upgrade During Install)] オプションを選択します。インストールの詳細については、『*Installation Guide for Cisco Unified Communications Manager and the IM and Presence Service*』を参照してください。

ステップ3 Cisco Unified CM をインストールしたら、その Cisco Unified CM のバージョンをサポートしているインストール マニュアルの説明に従って、後続のノードを設定します。

ステップ4 Cisco Unified Reporting、RTMT、または CLI にアクセスして、データベース レプリケーションが既存のノード間で発生していることを確認します。必要に応じて、ノード間のデータベース レプリケーションを修復します。

インストール前のクラスタへのノードの追加

ノードをインストールする前に、Cisco Unified Communications Manager Administration を使用して、新しいノードをクラスタに追加します。ノードの追加時に選択するサーバタイプは、インストールしたサーバタイプと一致する必要があります。

新しいノードをインストールする前に、Cisco Unified Communications Manager Administration を使用して、最初のノードで新しいノードを設定する必要があります。クラスタにノードをインストールするには、『*Cisco Unified Communications Manager Installation Guide*』を参照してください。

Cisco Unified Communications Manager のビデオ/音声サーバでは、Cisco Unified Communications Manager ソフトウェアの初期インストール中に追加した最初のサーバがパブリッシャノードに指定されます。後続のすべてのサーバインストールまたは追加は、サブスクライバ ノードに指定されます。クラスタに追加した最初の Cisco Unified Communications Manager IM and Presence ノードが、IM and Presence Service データベース パブリッシャノードに指定されます。



(注) サーバの追加後は、Cisco Unified Communications Manager Administration を使用して、サーバタイプを変更できなくなります。既存のサーバインスタンスを削除してから、再度、新しいサーバを追加して、正しいサーバタイプ設定を選択する必要があります。

手順

ステップ1 [システム (System)] > [サーバ (Server)] を選択します。

[サーバの検索/一覧表示 (Find and List Servers)] ウィンドウが表示されます。

ステップ 2 [新規追加 (Add New)] をクリックします。

[サーバの設定 - サーバを追加 (Server Configuration - Add a Server)] ウィンドウが表示されます。

ステップ 3 [サーバタイプ (Server Type)] ドロップダウンリスト ボックスで、追加するサーバタイプを選択してから、[次へ (Next)] をクリックします。

- CUCM ビデオ/音声
- CUCM IM and Presence

ステップ 4 [サーバの設定 (Server Configuration)] ウィンドウで、適切なサーバ設定を入力します。

サーバ設定フィールドの説明については、「[Server Settings](#)」を参照してください。

ステップ 5 [保存 (Save)] をクリックします。

プレゼンス サーバのステータスの表示

IM and Presence Service ノードの重要なサービスのステータスと自己診断テスト結果を確認するには、Cisco Unified Communications Manager Administration を使用します。

手順

ステップ 1 [システム (System)] > [サーバ (Server)] を選択します。

[サーバの検索/一覧表示 (Find and List Servers)] ウィンドウが表示されます。

ステップ 2 サーバの検索パラメータを選択し、[検索 (Find)] をクリックします。

一致するレコードが表示されます。

ステップ 3 [サーバの検索/一覧表示 (Find and List Servers)] ウィンドウに表示される IM and Presence サーバを選択します。

[サーバの設定 (Server Configuration)] ウィンドウが表示されます。

ステップ 4 [サーバの設定 (Server Configuration)] ウィンドウの IM and Presence サーバ情報のセクションで、プレゼンス サーバステータスのリンクをクリックします。

サーバの [ノードの詳細 (Node Details)] ウィンドウが表示されます。

ポートの設定

SCCPデバイス登録、SIPデバイス登録、MGCPゲートウェイ接続などの接続に使用されるポートの設定を変更するには、この手順を使用します。



- (注) 通常、デフォルトのポート設定を変更する必要はありません。この手順は、デフォルトを変更する場合にのみ使用します。

手順

- ステップ 1** Cisco Unified Communications Manager Administration で、[システム (System)] > [Cisco Unified CM] を選択します。
[Cisco Unified CM の検索と一覧表示 (Find and List Cisco Unified CMs)] ウィンドウが表示されます。
- ステップ 2** 適切な検索条件を入力し、[検索 (Find)] をクリックします。
一致するすべての Cisco Unified Communications Manager が表示されます。
- ステップ 3** 表示する Cisco Unified CM を選択します。
[Cisco Unified CM の設定 (Cisco Unified CM Configuration)] ウィンドウが表示されます。
- ステップ 4** [このサーバの Cisco Unified Communications Manager TCP ポートの設定 (Cisco Unified Communications Manager TCP Port Settings for this Server)] セクションに移動します。
- ステップ 5** Cisco Unified Communications Manager のポートを設定します。
フィールドとその設定オプションの詳細については、「[ポート設定 \(322 ページ\)](#)」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** [設定の適用 (Apply Config)] をクリックします。
- ステップ 8** [OK] をクリックします。

ポート設定

フィールド	説明
[イーサネット電話ポート (Ethernet Phone Port)]	<p>システムは、このTCPポートを使用してネットワークのCisco Unified IP Phone (SCCP 専用) と通信します。</p> <ul style="list-style-type: none"> このポートがシステムですでに使用中でない限り、デフォルトポートの値 2000 を受け入れます。2000 を選択すると、このポートは非セキュアとして識別されます。 すべてのポートエントリが一意であることを確認してください。 有効なポート番号の範囲は 1024 ~ 49151 です。
[MGCPリッスンポート (MGCP Listen Port)]	<p>システムは、TCPポートを使用して、その関連するMGCPゲートウェイからのメッセージを検出する。</p> <ul style="list-style-type: none"> このポートがシステムですでに使用中でない限り、デフォルトポート 2427 を受け入れます。 すべてのポートエントリが一意であることを確認してください。 有効なポート番号の範囲は 1024 ~ 49151 です。
[MGCPキープアライブポート (MGCP Keep-alive Port)]	<p>システムは、このTCPポートを使用して、その関連するMGCPゲートウェイとアクティブメッセージを交換する。</p> <ul style="list-style-type: none"> このポートがシステムですでに使用中でない限り、デフォルトポート 2428 を受け入れます。 すべてのポートエントリが一意であることを確認してください。 有効なポート番号の範囲は 1024 ~ 49151 です。
[SIP電話ポート (SIP Phone Port)]	<p>このフィールドでは、Unified Communications Manager が TCP と UDP を介して SIP 回線登録をリッスンするのに使用するポート番号を指定します。</p>
[SIP電話セキュアポート (SIP Phone Secure Port)]	<p>このフィールドでは、システムが TLS を介して SIP 回線登録をリッスンするのに使用するポート番号を指定します。</p>
SIP 電話 OAuth ポート (SIP Phone OAuth Port)	<p>このフィールドは、Cisco Unified Communications Manager が TLS (Transport Layer Security) を介して、オンプレミスの Jabber デバイスによる SIP 回線への登録をリッスンするために使用するポート番号を指定します。デフォルト値は 5090 です。範囲は 1024 ~ 49151 です。</p>

フィールド	説明
SIPモバイルおよびリモートアクセスOAuthポート	このフィールドでは、Cisco Unified Communications Manager が MTL S (Mutual Transport Layer Security) を介して Expressway 上の Jabber からの SIP 回線登録を受信するために使用するポート番号を指定します。デフォルト値は 5091 です。範囲は 1024 ~ 49151 です。

ホスト名の設定

次の表に、Unified Communications Manager サーバのホスト名を設定できる場所、ホスト名として指定できる文字数、および推奨されるホスト名の先頭文字と最終文字を示します。ホスト名を正しく設定しないと、Unified Communications Manager の一部のコンポーネント（オペレーティングシステム、データベース、インストールなど）が期待通りに機能しない可能性があります。

表 74: Cisco Unified Communications Manager におけるホスト名の設定

ホスト名の場所	可能な設定	指定できる文字数	推奨されるホスト名の先頭文字	推奨されるホスト名の最終文字
[ホスト名/IP アドレス (Host Name/IP Address)] フィールド Cisco Unified Communications Manager Administration の [システム (System)] > [サーバ (Server)]	クラスタ内のサーバのホスト名を追加または変更できます。	2 ~ 63	英字	英数字
[ホスト名 (Hostname)] フィールド Cisco Unified Communications Manager インストール ウィザード	クラスタ内のサーバのホスト名を追加できます。	1 ~ 63	英字	英数字
[ホスト名 (Hostname)] フィールド Cisco Unified Communications オペレーティング システム の [設定 (Settings)] > [IP] > [イーサネット (Ethernet)]	クラスタ内のサーバのホスト名を変更できますが、追加はできません。	1 ~ 63	英字	英数字
set network hostname hostname コマンドライン インターフェイス	クラスタ内のサーバのホスト名を変更できますが、追加はできません。	1 ~ 63	英字	英数字



ヒント このホスト名は、ARPANET ホスト名の規則に従う必要があります。ホスト名の先頭文字と最終文字の間には、英数文字とハイフンを入力できます。

いずれかの場所でホスト名を設定する前に、次の情報を確認してください。

- [サーバの設定 (Server Configuration)] ウィンドウの [ホスト名/IP アドレス (Host Name/IP Address)] フィールドは、デバイスとサーバ間、アプリケーションとサーバ間、および異なるサーバ間の通信をサポートします。このフィールドには、ドット区切り形式の IPv4 アドレスまたはホスト名を入力できます。

Unified Communications Manager パブリッシャ ノードをインストールした後は、パブリッシャのホスト名がこのフィールドに自動的に表示されます。Unified Communications Manager サブスクライバノードをインストールする前に、Unified Communications Manager パブリッシャ ノードでこのフィールドにサブスクライバノードの IP アドレスまたはホスト名を入力してください。

このフィールドにホスト名を設定できるのは、Unified Communications Manager が DNS サーバにアクセスしてホスト名を IP アドレスに解決できる場合のみです。DNS サーバに Cisco Unified Communications Manager の名前とアドレスの情報が設定されていることを確認してください。



ヒント DNS サーバに Unified Communications Manager の情報を設定するのに加えて、Cisco Unified Communications Manager のインストール時に DNS 情報を入力します。

- Unified Communications Manager パブリッシャ ノードのインストール時に、ネットワーク情報を設定するために (つまり、スタティック ネットワークを使用する場合に) パブリッシャ サーバのホスト名 (必須) と IP アドレスを入力します。

Unified Communications Manager サブスクライバノードのインストール時には、Unified Communications Manager パブリッシャ ノードのホスト名と IP アドレスを入力して、Unified Communications Manager がネットワークの接続性およびパブリッシャとサブスクライバ間の検証を確認できるようにしてください。さらに、サブスクライバ ノードのホスト名と IP アドレスも入力する必要があります。Unified Communications Manager のインストール時にサブスクライバ サーバのホスト名の入力を求められた場合は、Cisco Unified Communications Manager Administration の ([ホスト名/IP アドレス (Host Name/IP Address)] フィールドでサブスクライバサーバのホスト名を設定した場合に) [サーバの設定 (Server Configuration)] ウィンドウに表示される値を入力します。

Kerneldump ユーティリティ

Kerneldump ユーティリティにより、セカンダリ サーバを要求することなしに、該当するマシンでクラッシュ ダンプ ログをローカルに収集できます。

Unified Communications Manager クラスタでは、Kerneldump ユーティリティがサーバで有効であることを確認するだけで、クラッシュ ダンプ情報を収集できます。



- (注) シスコでは、より効果的なトラブルシューティングを実現するため、Unified Communications Manager のインストール後に、Kerneldump ユーティリティが有効であることを確認するよう推奨しています。Kerneldump ユーティリティの設定をまだ行っていない場合は、Unified Communications Manager をサポート対象のアプライアンスリリースからアップグレードする前に行ってください。



- 重要** Kerneldump ユーティリティをイネーブル化またはディセーブル化を行うには、ノードのリブートが必要です。リブートが許容されるウィンドウ以外では、enable コマンドを実行しないでください。

Cisco Unified Communications オペレーティング システムのコマンドライン インターフェイス (CLI) を使用すると、Kerneldump ユーティリティのイネーブル化、ディセーブル化、ステータス確認を実行できます。

次の手順を利用して Kerneldump ユーティリティをイネーブル化します。

ユーティリティによって収集されるファイルの処理

Kerneldump ユーティリティから送信されたクラッシュ情報を表示するには、Cisco Unified Real-Time Monitoring Tool またはコマンドライン インターフェイス (CLI) を使用します。Cisco Unified Real-Time Monitoring Tool を使用して netdump ログを収集するには、[トレースおよびログ セントラル (Trace & Log Central)] の [ファイルの収集 (Collect Files)] オプションを選択します。[システム サービス/アプリケーションの選択 (Select System Services/Applications)] タブで、[Kerneldump ログ (Kerneldump logs)] チェックボックスをオンにします。Cisco Unified Real-Time Monitoring Tool を使用したファイルの収集の詳細については、『Cisco Unified Real-Time Monitoring Tool Administration Guide』を参照してください。

CLI を使用して kerneldump ログを収集するには、クラッシュ ディレクトリのファイルに対して「file」 CLI コマンドを使用します。これらは「active-log」のパーティションの下にあります。ログ ファイル名は、kerneldump クライアントの IP アドレスで始まり、ファイルが作成された日付で終わります。ファイル コマンドの詳細については、『Command Line Interface Reference Guide for Cisco Unified Solutions』を参照してください。

Kerneldump ユーティリティの有効化

次の手順を利用して Kerneldump ユーティリティをイネーブル化します。カーネル クラッシュが発生した場合、ユーティリティは、クラッシュの収集とダンプのメカニズムを提供します。ローカル サーバまたは外部サーバにログをダンプするユーティリティを設定できます。

手順

ステップ 1 コマンドライン インターフェイスにログインします。

ステップ 2 次のいずれかを実行します。

- ローカルサーバ上のカーネルクラッシュをダンプするには、`utils os kernelcrash enable` CLI コマンドを実行します。
- 外部サーバにカーネルクラッシュをダンプするには、外部サーバの IP アドレスを指定して `utils os kerneldump ssh enable <ip_address>` CLI コマンドを実行します。

ステップ 3 サーバをリブートします。

例



(注) `kerneldump` ユーティリティを無効にする必要がある場合、`utils os kernelcrash disable` CLI コマンドを実行してローカルサーバのコア ダンプを無効にし、`utils os kerneldump ssh disable <ip_address>` CLI コマンドを実行して外部サーバ上のユーティリティを無効にします。

次のタスク

コア ダンプの指示に従ってリアルタイム モニタリング ツールで電子メールアラートを設定します。詳細については、[コア ダンプの電子メールアラートの有効化 \(326ページ\)](#) を参照してください。

`kerneldump` ユーティリティおよびトラブルシューティングについては、『*Troubleshooting Guide for Cisco Unified Communications Manager*』を参照してください。

コア ダンプの電子メール アラートの有効化

コア ダンプが発生するたびに管理者に電子メールを送信するようにリアルタイム モニタリング ツールを設定するには、次の手順を使用します。

手順

ステップ 1 [システム (System)]>[ツール (Tools)]>[アラート セントラル) Alert Central)] の順に選択します。

ステップ 2 [CoreDumpFileFound] アラートを右クリックし、[アラート/プロパティの設定 (Set Alert/Properties)] を選択します。

ステップ 3 ウィザードの指示に従って優先条件を設定します。

- a) [アラート プロパティ：電子メール通知 (Alert Properties: Email Notification)] ポップアップで、[電子メールの有効化 (Enable Email)] がオンになっていることを確認し、[設定 (Configure)] をクリックしてデフォルトのアラート アクションを設定します。これにより管理者に電子メールが送信されます。
- b) プロンプトに従って、受信者電子メールアドレスを [追加 (Add)] します。このアラートがトリガーされると、デフォルトのアクションは、このアドレスへの電子メールの送信になります。
- c) [保存 (Save)] をクリックします。

ステップ 4 デフォルトの電子メール サーバを設定します。

- a) [システム (System)] > [ツール (Tools)] > [アラート (Alert)] > [電子メール サーバの設定 (Config Email Server)] の順に選択します。
- b) 電子メールアラートを送信する電子メールサーバーとポート情報を入力します。
- c) (オプション) SMTP サーバーへの暗号化された通信チャネルを有効にするには、[TLS モードの有効化 (Enable TLS mode)] チェックボックスをオンにします。
- d) (オプション) 受信者の電子メールアドレスの認証を要求するには、[認証モードの有効化 (Enable Authentication mode)] チェック ボックスをオンにします。
(注) [ユーザー名 (Username)] および [パスワード (Password)] フィールドにアクセスできるのは、[認証モードの有効化 (Enable Authentication mode)] チェック ボックスが有効になっている場合のみです。
- e) [Username] フィールドにユーザー名を入力します。
- f) パスワードを [Password] フィールドに入力します。
- g) [送信するユーザー ID (Send User ID)] を入力します。
- h) [OK] をクリックします。



第 **V** 部

レポートの管理

- [Cisco Serviceability Reporter](#) (331 ページ)
- [Cisco Unified Reporting](#) (351 ページ)
- [Cisco IP Phone 電話の通話診断と品質レポートを設置する](#) (365 ページ)



第 21 章

Cisco Serviceability Reporter

- サービスアビリティ レポートのアーカイブ (331 ページ)
- Cisco Serviceability Reporter 設定タスク フロー (332 ページ)
- 日次レポートの概要 (334 ページ)

サービスアビリティ レポートのアーカイブ

Cisco 有用性 Reporter サービスは、特定のレポートの統計情報の要約を表示するチャートを含む日次レポートを生成します。Reporter は、ログに記録された情報に基づいてレポートを 1 日 1 回生成します。

有用性 GUI を使用して、**ツール > 有用性レポートアーカイブ**からレポートを表示します。レポートを表示する前に、Cisco Serviceability Reporter サービスをアクティブ化する必要があります。サービスをアクティブ化した後、レポートの生成に最大 24 時間かかる場合があります。

レポートには、前日の 24 時間のデータが含まれます。レポート名に追加されるサフィックスは、Reporter がレポートを生成した日付を表します。たとえば、AlertRep_mm_dd_yyyy.pdf です。[サービスアビリティ レポートのアーカイブ (Serviceability Reports Archive)] ウィンドウでは、この日付を使用して該当する日付だけのレポートを表示します。レポートは、前日のタイムスタンプを持つログファイルにあるデータから生成されます。システムは、現在の日付と過去 2 日間のログ ファイルを対象にデータを収集します。

レポートに表示される時刻は、サーバの「システム時刻」が反映されます。

レポートの生成中に、サーバからログファイルを取得できます。



- (注) Cisco Unified Reporting Web アプリケーションは、1つの出力にデータのスナップショットビューを提供し、データチェックを実行します。また、生成されたレポートをアーカイブすることもできます。詳細については、『Cisco Unified Reporting アドミニストレーションガイド』を参照してください。

クラスタ設定の有用性レポートアーカイブの考慮事項

この項では、Unified Communications Manager および IM and Presence Service のみに適用されません。

- Cisco Serviceability Reporter は最初のサーバでのみアクティブなため、Reporter は常に、他のサーバではなく、最初のサーバでのみレポートを生成します。
- レポートに表示される時刻には、最初のサーバの「システム時刻」が反映されます。最初のサーバとそれに続くサーバが異なる時間帯に設置されている場合は、最初のサーバの「システム時刻」がレポートに表示されます。
- クラスタ内のサーバロケーション間のタイムゾーンの違いは、レポートのデータが収集されるときに考慮されます。
- レポートを生成するときに、個々のサーバまたはクラスタ内のすべてのサーバからログファイルを選択できます。
- シスコのユニファイドレポートング Web アプリケーションの出力およびデータチェックには、すべてのアクセス可能なサーバからのクラスタデータが含まれます。

Cisco Serviceability Reporter 設定タスク フロー

これらのタスクを実行して、シスコの有用性レポーターを通じて、毎日のシステムレポートを設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	Cisco Serviceability Reporter のアクティブ化 (332 ページ)	日次レポートを生成するためには、 Cisco Serviceability Reporter サービスが実行されている必要があります。
ステップ 2	Cisco Serviceability Reporter の設定 (333 ページ)	シスコの有用性レポーターのスケジューリング設定を行います。
ステップ 3	日次レポート アーカイブの表示 (334 ページ)	システムが日次レポートを生成したら、このタスクを使用して、PDF ファイル内の日次レポートを表示します。

Cisco Serviceability Reporter のアクティブ化

この手順を使用して、シスコの有用性レポーターで毎日のシステムレポートを有効にします。生成するレポートの場合は、サービスを**アクティブ**にする必要があります。

手順

- ステップ 1 Cisco Unified Serviceability から、[ツール (Tools)] > [サービスのアクティブ化 (Service Activation)] を選択します。
- ステップ 2 サーバを選択し、[Go (移動)] をクリックします。
- ステップ 3 [Performance And Monitoring Services] で、Cisco 有用性 Reporter サービスのステータスを確認します。
- ステップ 4 サービスが非アクティブ化されている場合は、隣接するオプションボタンにチェックを入れ、[保存 (Save)] をクリックします。



- (注) レポートは毎日生成されます。最初のレポートが生成されるまでに、最大で24時間かかる場合があります。

Cisco Serviceability Reporter の設定

シスコの有用性レポーターが生成する日次レポートのスケジューリング設定を構成します。

手順

- ステップ 1 Cisco Unified CM Administration から、[システム (System)] > [サービス パラメータ (Service Parameters)] の順に選択します。
- ステップ 2 シスコの有用性レポーターが実行されているサーバを選択します。
- ステップ 3 [サービス (Service)] ドロップダウン リストから、[Cisco Serviceability Reporter] を選択します。
- ステップ 4 次のサービス パラメータを設定します。
 - **RTMT Reporter Designated Node** : RTMT Reporter が動作する指定ノードを指定します。シスコでは、非呼処理ノードを割り当てることを推奨しています。
 - **レポート生成時間**: レポートが生成する午前零時からの経過時間 (分単位)。指定できる範囲は 0 ~ 1439 で、デフォルト設定は 30 分です。
 - **レポート削除経過時間**: レポートがディスクに保存される日数。範囲は 0-30 で、デフォルト設定は 7 日です。
- ステップ 5 [保存 (Save)] をクリックします。

日次レポート アーカイブの表示

シスコの有用性レポーターが日次レポートを生成している場合は、次の手順を使用して PDF ファイル内のレポートを表示します。

手順

ステップ 1 [ツール (Tools)] > [サービスアビリティ レポートのアーカイブ (Serviceability Reports Archive)] を選択します。

ステップ 2 レポートを表示する月と年を選択します。
選択した月に対応する日の一覧が表示されます。

ステップ 3 生成されたレポートを表示する日付をクリックします。

ステップ 4 表示したいレポートをクリックします。

(注) PDF 形式でレポートを表示するには、Acrobat Reader をインストールしてください。Acrobat Reader をダウンロードするには、[Serviceability Reports Archive] ウィンドウの下部にあるリンクをクリックします。

日次レポートの概要

Cisco Serviceability Reporter によって、次のシステム レポートが毎日生成されます。

- デバイス統計レポート
- サーバ統計レポート
- サービス統計レポート
- コール アクティビティ レポート
- アラート要約レポート
- パフォーマンス保護レポート

デバイス統計レポート

デバイス統計情報レポートは、IM and Presence サービスおよびCisco Unity Connectionには適用されません。

デバイス統計レポートでは、次の折れ線グラフが表示されます。

- サーバごとの登録済み電話機の数
- クラスタ内の H.323 ゲートウェイの数

- クラスタ内のトランクの数

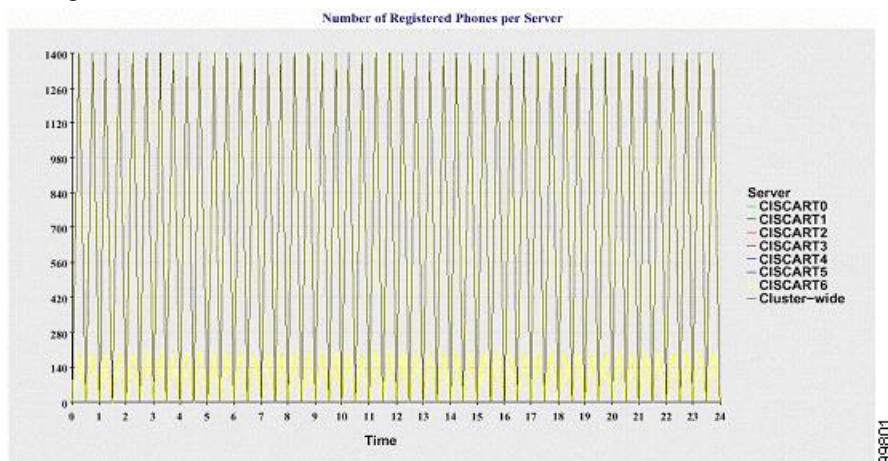
サーバごとの登録済み電話機の数

折れ線グラフには、Unified Communications Manager の各サーバ（および Unified Communications Manager クラスタ構成のクラスタ）に登録された電話機の数が表示されます。グラフの各線はデータが利用できるサーバのデータを表し、もう 1 本はクラスタ全体のデータを示します

（Unified Communications Manager クラスタのみ）。グラフ内の各データ値は、15 分の間に登録された電話機の平均数を表します。サーバにデータが表示されない場合、そのサーバを表す線は生成されません。データがサーバ（または Unified Communications Manager クラスタ構成のすべてのサーバ）に存在しない場合、Reporter はグラフを生成しません。「利用可能なデバイス統計レポートのデータがありません」のメッセージが表示されます。

図 4: サーバごとの登録済み電話機の数を示す折れ線グラフ

以下の図では、Unified Communications Manager のクラスタ構成内の Unified Communications Manager サーバごとの登録済み電話機の数を表す折れ線グラフの例を示しています。

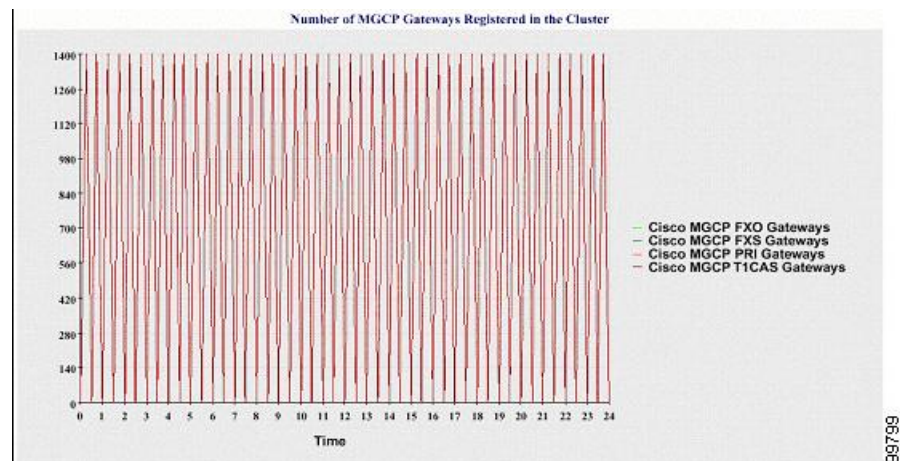


クラスタ内の登録済み MGCP ゲートウェイの数

折れ線グラフには、登録済み MGCP FXO、FXS、PRI、T1CAS ゲートウェイの数が表示されます。各線は、Unified Communications Manager サーバ（または Unified Communications Manager クラスタ構成のクラスタ）のデータだけを表します。つまり、4 本の線は各ゲートウェイタイプのサーバ（またはクラスタ全体）の詳細を示します。グラフ内の各データ値は、15 分の間に登録された MGCP ゲートウェイの平均数を表します。あるゲートウェイに関するデータがサーバ（またはクラスタ内のすべてのサーバ）に存在しない場合、そのゲートウェイのデータを表す線は生成されません。すべてのゲートウェイに関するデータがサーバ（またはクラスタ内のすべてのサーバ）に存在しない場合、グラフは生成されません。

図 5: クラスタごとの登録済みゲートウェイの数を示す折れ線グラフ

次の図は、Unified Communications Manager クラスタ構成におけるクラスタごとの登録済みゲートウェイの数を表す折れ線グラフの例を示しています。

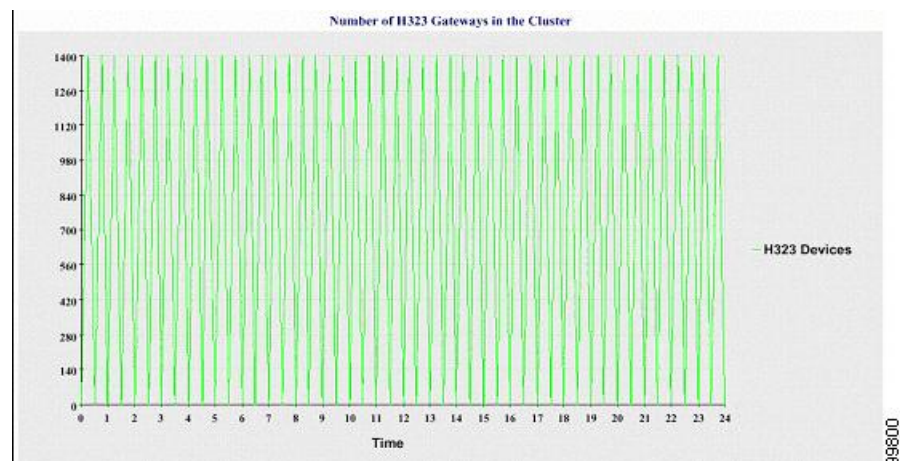


クラスタ内の H.323 ゲートウェイの数

折れ線グラフには、H.323 ゲートウェイの数が表示されます。1本の線は、H.323 ゲートウェイの詳細（あるいは Unified Communications Manager のクラスタ構成のクラスタ全体の詳細）を示しています。グラフ内の各データ値は、15分間での H.323 ゲートウェイの平均数を表します。サーバ（またはクラスタ内のすべてのサーバ）の H.323 ゲートウェイに関するデータが存在しない場合、グラフは生成されません。

図 6: クラスタごとの登録済み H.323 ゲートウェイの数を示す折れ線グラフ

次の図は、Unified Communications Manager クラスタ構成のクラスタごとの H.323 ゲートウェイの数を表す折れ線グラフの例を示しています。



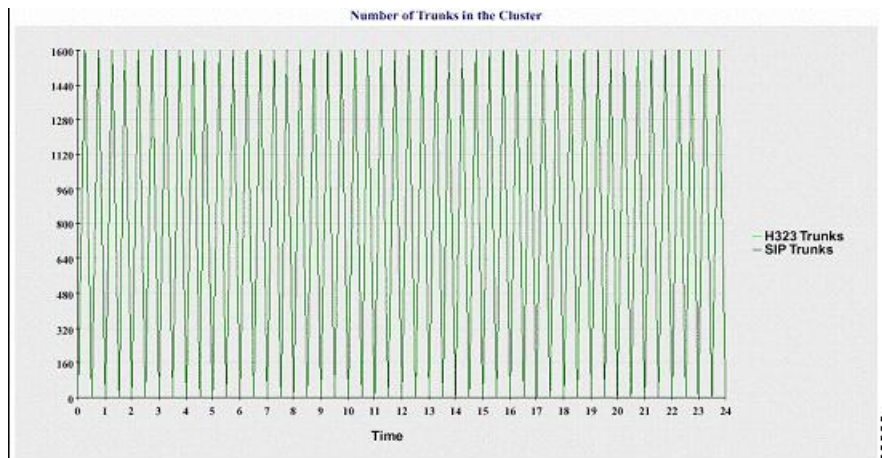
クラスタ内のトランクの数

折れ線グラフには、H.323 および SIP トランクの数が表示されます。2本の線が、H.323 トランクおよび SIP トランクの詳細（または Unified Communications Manager のクラスタ構成のクラスタ全体の詳細）を示します。グラフ内の各データ値は、15分間での H.323 および SIP トランクの平均数を表します。サーバ（またはクラスタ内のすべてのサーバ）の H.323 トランクに関するデータが存在しない場合、H.323 トランクのデータを表す線は生成されません。サーバ（ま

たはクラスタ内のすべてのサーバ) の SIP トランクに関するデータが存在しない場合、SIP トランクのデータを表す線は生成されません。トランクに関するデータがまったく存在しない場合、グラフは生成されません。

図 7: クラスタごとのトランクの数を示す折れ線グラフ

次の図は、Unified Communications Manager クラスタ構成のクラスタごとのトランクの数を表す折れ線グラフの例を示します。



サーバ (またはクラスタ内の各サーバ) には、ファイル名パターン DeviceLog_mm_dd_yyyy_hh_mm.csv に一致するログファイルが格納されています。ログファイルには次の情報が格納されています。

- サーバ (または Unified Communications Manager クラスタ内の各サーバ) 上の登録済み電話機の数
- サーバ (または Unified Communications Manager クラスタ内の各サーバ) 上の登録済み MGCP FXO、FXS、PRI、および T1CAS ゲートウェイの数
- サーバ (または Unified Communications Manager クラスタ内の各サーバ) 上の登録済み H.323 ゲートウェイの数
- SIP トランクと H.323 トランクの数

サーバ統計レポート

サーバ統計レポートでは、次の折れ線グラフが表示されます。

- サーバごとの CPU のパーセンテージ
- サーバごとのメモリ使用率のパーセンテージ
- サーバごとの最大パーティションのハードディスク使用率のパーセンテージ

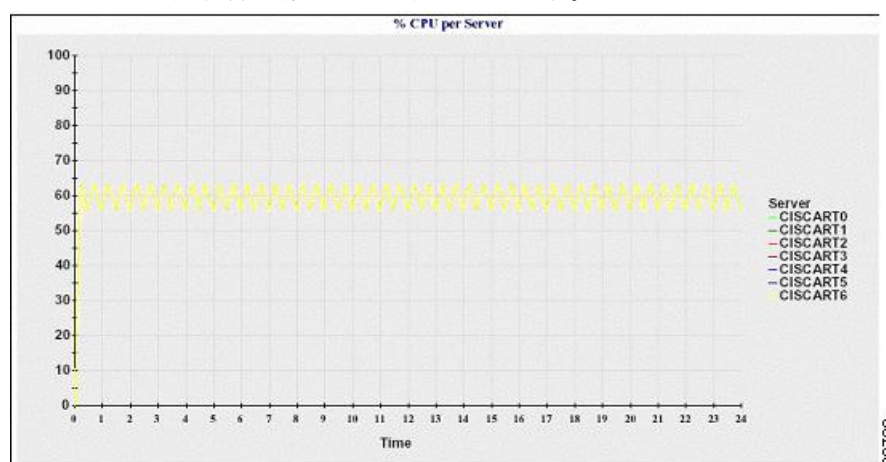
クラスタ固有の統計情報は、Unified Communications Manager および IM and Presence Serviceでのみサポートされます。

サーバごとの CPU のパーセンテージ

折れ線グラフには、サーバ（またはクラスタ内の各サーバ）の CPU 使用率のパーセンテージが表示されます。グラフの折れ線は、データが利用できるサーバのデータを表します（または、クラスタ内のサーバごとに1本の折れ線）。グラフ内の各データ値は、15分間の平均CPU使用率を表します。サーバ（またはクラスタ内のいずれかのサーバ）のデータが存在しない場合、そのサーバを表す線は生成されません。生成する線がない場合は、Reporter はグラフを作成しません。「利用可能なサーバ統計レポートのデータがありません」のメッセージが表示されます。

図 8: サーバごとの CPU のパーセンテージを示す折れ線グラフ

次の図は、Unified Communications Manager のクラスタ構成でサーバごとの CPU 使用率のパーセンテージを表す折れ線グラフの例を示します。

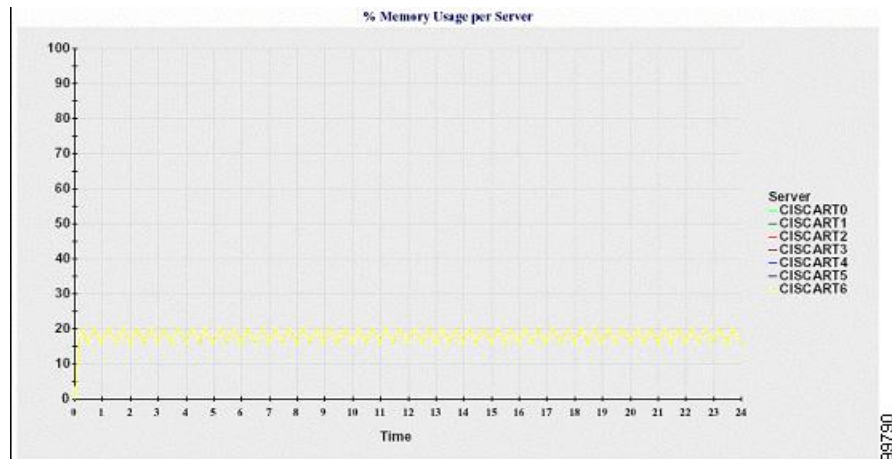


サーバごとのメモリ使用率のパーセンテージ

折れ線グラフには、Unified Communications Manager サーバのメモリ使用率のパーセンテージ (%MemoryInUse) が表示されます。Unified Communications Manager クラスタ構成では、データが利用できるクラスタ内のサーバごとに1本の線があります。グラフ内の各データ値は、15分間の平均メモリ使用率を表します。データが存在しない場合はグラフが生成されません。クラスタ構成でいずれかのサーバのデータが存在しない場合、Reporter はそのサーバを表す線を生成しません。

図 9: サーバごとのメモリ使用率のパーセンテージを示す折れ線グラフ

次の図は、クラスタ構成で Unified Communications Manager サーバあたりのメモリ消費率を示す線グラフの例を示します。

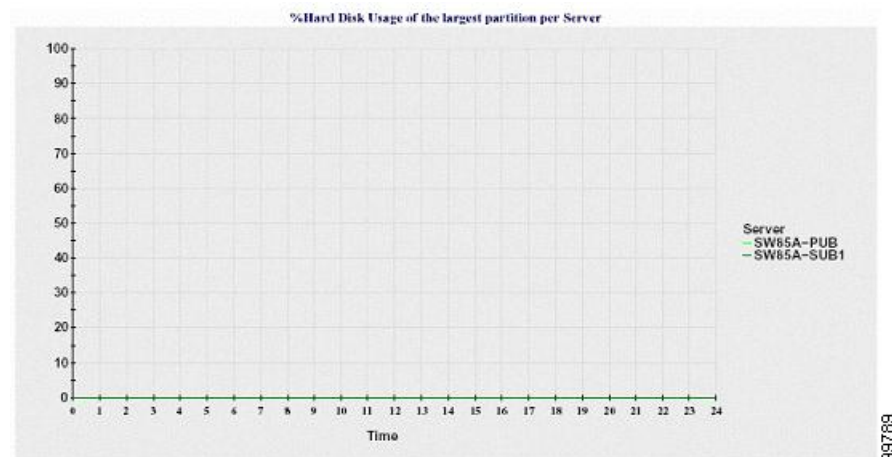


サーバごとの最大パーティションのハードディスク使用率のパーセンテージ

折れ線グラフには、サーバまたはクラスタ構成の各サーバ上の最大パーティションのディスク領域使用率のパーセンテージ (%DiskSpaceInUse) が表示されます。グラフ内の各データ値は、15 分間の平均ディスク使用率を表します。データが存在しない場合はグラフが生成されません。クラスタ構成でいずれかのサーバのデータが存在しない場合、Reporter はそのサーバを表す線を生成しません。

図 10: サーバごとの最大パーティションのハードディスク使用率のパーセンテージを示す折れ線グラフ

次の図は、Unified Communications Manager のクラスタ構成でサーバごとの最大パーティションのハードディスク使用率のパーセンテージを表す折れ線グラフの例を示します。



サーバ（またはクラスタ構成内の各サーバ）には、ファイル名パターン `ServerLog_mm_dd_yyyy_hh_mm.csv` に一致するログファイルが格納されています。ログファイルには次の情報が格納されています。

- サーバ（またはクラスタ内の各サーバ）での CPU 使用率
- サーバ（またはクラスタ内の各サーバ）でのメモリ使用率 (%MemoryInUse)

- サーバ（またはクラスタの各サーバ）の最大パーティションのハードディスク使用率（%DiskSpaceInUse）

サービス統計レポート

サービス統計レポートは、IM and Presence Service および Cisco Unity Connection をサポートしていません。

サービス統計レポートでは、次の折れ線グラフが表示されます。

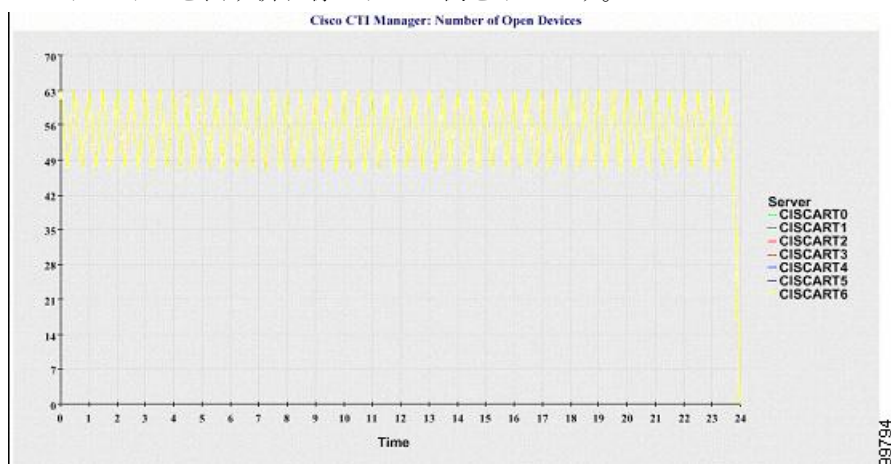
- Cisco CTI Manager : オープン デバイスの数
- Cisco CTI Manager : オープン回線の数
- Cisco TFTP : 要求の数
- Cisco TFTP : 中断された要求の数

Cisco CTI Manager : オープン デバイスの数

折れ線グラフには、CTI Manager（または Unified Communications Manager クラスタ構成内の各 CTI Manager）の CTI オープン デバイスの数が表示されます。各折れ線グラフは、サービスがアクティブなサーバ（または Unified Communications Manager のクラスタ内の各サーバ）のデータを表します。グラフ内の各データ値は、15 分間の CTI オープン デバイスの平均数を表します。データが存在しない場合はグラフが生成されません。Unified Communications Manager クラスタ構成でいずれかのサーバのデータが存在しない場合、Reporter はそのサーバを表す線を生成しません。「利用可能なサービス統計レポートのデータがありません」のメッセージが表示されます。

図 11: Cisco CTI Manager : オープン デバイスの数を示す折れ線グラフ

次の図は、Unified Communications Manager のクラスタ構成で Cisco CTI Manager あたりのオープン デバイスを表す折れ線グラフの例を示します。

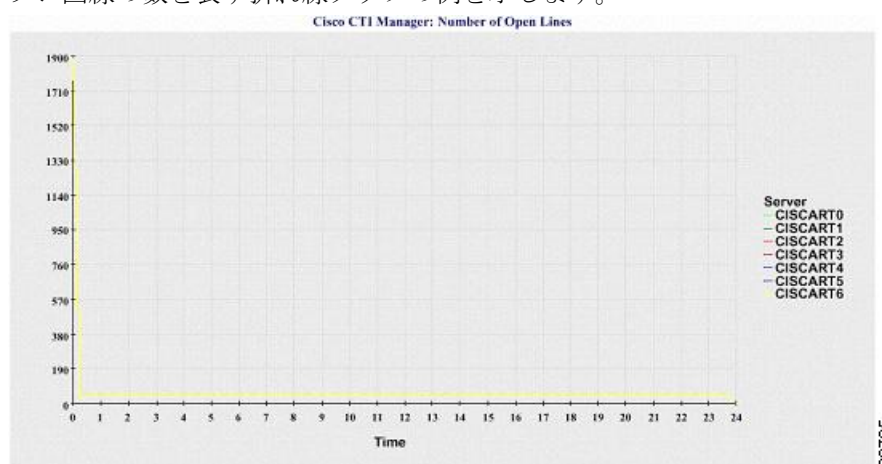


Cisco CTI Manager : オープン回線の数

折れ線グラフには、CTI Manager（または Unified Communications Manager クラスタ構成内の CTI Manager ごと）の CTI オープン回線の数が表示されます。グラフの折れ線は、Cisco CTI Manager サービスがアクティブなサーバのデータを表します（または Unified Communications Manager クラスタ構成内のサーバごとに 1 本の線）。グラフ内の各データ値は、15 分間の CTI オープン回線の平均数を表します。データが存在しない場合はグラフが生成されません。Unified Communications Manager クラスタ構成でいずれかのサーバのデータが存在しない場合、Reporter はそのサーバを表す線を生成しません。

図 12: Cisco CTI Manager : オープン回線の数を示す折れ線グラフ

次の図は、Unified Communications Manager のクラスタ構成内の Cisco CTI Manager ごとのオープン回線の数を表す折れ線グラフの例を示します。

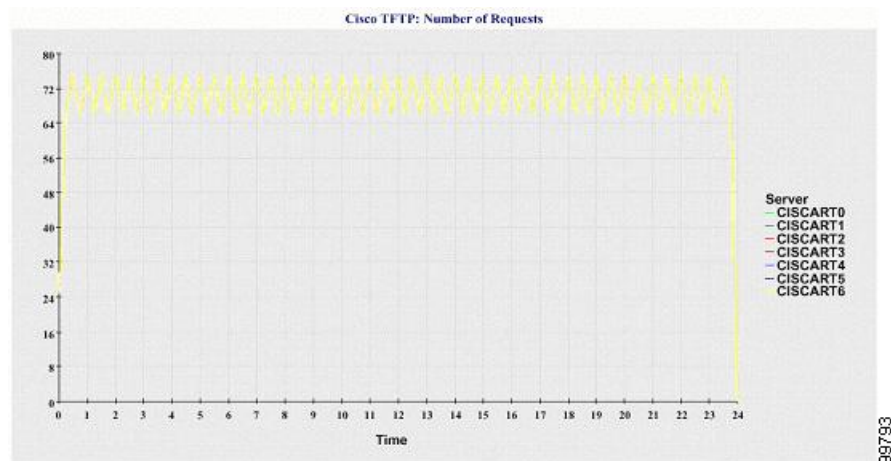


Cisco TFTP : 要求の数

折れ線グラフには、TFTP サーバ（または Unified Communications Manager クラスタ構成内の TFTP サーバごと）の Cisco TFTP 要求の数が表示されます。グラフの折れ線は、Cisco TFTP サービスがアクティブなサーバのデータを示します（または Unified Communications Manager クラスタ内のサーバごとに 1 本の線）。グラフ内の各データ値は、15 分間の TFTP 要求の平均数を表します。データが存在しない場合はグラフが生成されません。Unified Communications Manager クラスタ構成でいずれかのサーバのデータが存在しない場合、Reporter はそのサーバを表す線を生成しません。

図 13: Cisco TFTP : 要求の数を示す折れ線グラフ

次の図は、TFTP サーバごとの Cisco TFTP 要求の数を表す折れ線グラフの例を示します。

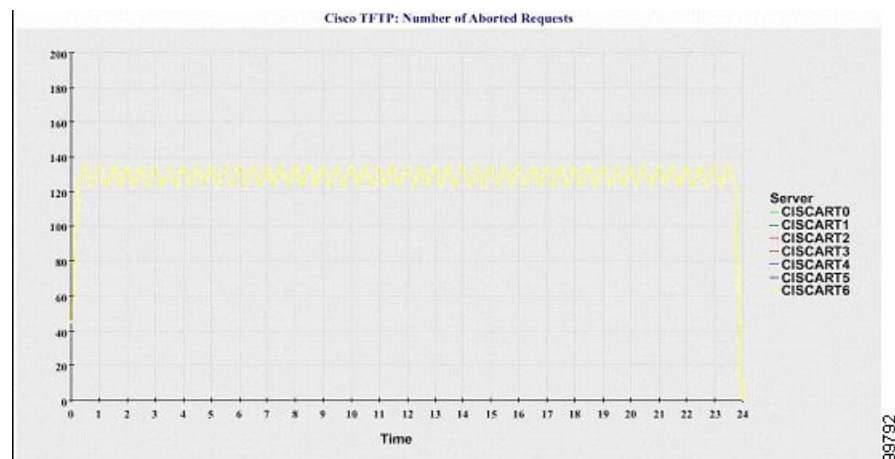


Cisco TFTP : 中断された要求の数

折れ線グラフには、TFTP サーバ（または Unified Communications Manager クラスタ構成内の TFTP サーバごと）の中断された Cisco TFTP 要求の数が表示されます。グラフの折れ線は、Cisco TFTP サービスがアクティブなサーバのデータを示します（または Unified Communications Manager クラスタ内のサーバごとに 1 本の線）。グラフ内の各データ値は、15 分間の中断された TFTP 要求の平均を表します。データが存在しない場合はグラフが生成されません。Unified Communications Manager クラスタ構成でいずれかのサーバのデータが存在しない場合、Reporter はそのサーバを表す線を生成しません。

図 14: Cisco TFTP : 中断された要求の数を示す折れ線グラフ

次の図は、TFTP サーバごとに中断された Cisco TFTP 要求の数を表す折れ線グラフの例を示します。



サーバ（または Unified Communications Manager クラスタ内の各サーバ）には、ファイル名パターン ServiceLog_mm_dd_yyyy_hh_mm.csv に一致するログ ファイルが格納されています。ログ ファイルには次の情報が格納されています。

- 各 CTI Manager : オープン デバイスの数

- 各 CTI Manager : オープン回線の数
- 各 Cisco TFTP サーバ : TotalTftpRequests
- 各 Cisco TFTP サーバ : TotalTftpRequestsAborted

コール アクティビティ レポート

コール アクティビティ レポートは、IM and Presence Service および Cisco Unity Connection をサポートしていません。

コール アクティビティ レポートでは、次の折れ線グラフが表示されます。

- クラスタの Unified Communications Manager コール アクティビティ
- クラスタの H.323 ゲートウェイ コール アクティビティ
- クラスタの MGCP ゲートウェイ コール アクティビティ
- MGCP ゲートウェイ
- クラスタのトランクコールアクティビティ

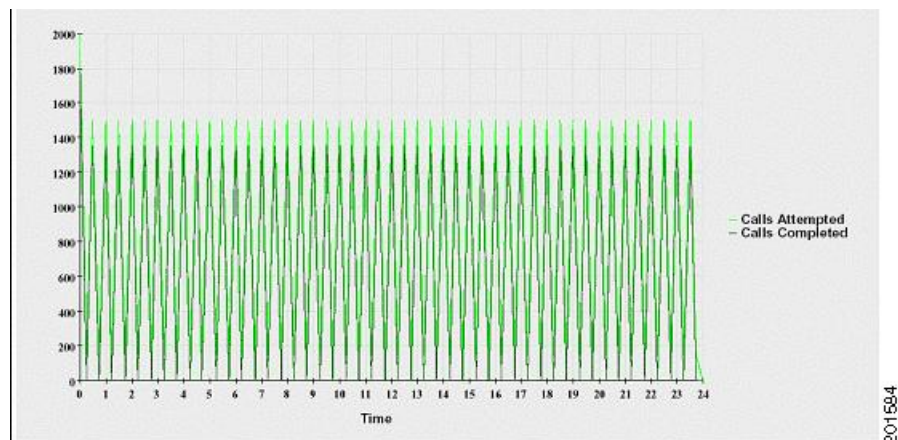
クラスタの Cisco Unified Communications Manager コール アクティビティ

折れ線グラフには、Unified Communications Manager の試行されたコールと完了したコールの数が表示されます。Unified Communications Manager のクラスタ構成では、折れ線グラフはクラスタ全体の試行されたコールと完了したコールの数を表します。グラフは2本の線で構成されます。1本は試行されたコールの数、もう1本は完了したコールの数を示します。Unified Communications Manager のクラスタ構成では、各線はクラスタ値を表します。これは（データが利用できる）クラスタ内のすべてのサーバの値の合計です。グラフ内の各データ値は、15分間に試行されたコールと完了したコールの総数を表します。

完了した Unified Communications Manager のコールのデータがない場合、Reporter は完了したコールのデータを表す線を生成しません。試行された Unified Communications Manager コールのデータが存在しない場合、試行されたコールのデータを表す線は生成されません。Unified Communications Manager のクラスタ構成では、クラスタ内のサーバのデータがない場合、Reporter はそのサーバで試行されたコールまたは完了したコールを表す線を生成しません。Unified Communications Manager コールアクティビティのデータがまったく存在しない場合、グラフは生成されません。「利用可能なコールアクティビティレポートのデータがありません」のメッセージが表示されます。

図 15: クラスタの Cisco Unified Communications Manager コール アクティビティを示す折れ線グラフ

次の図は、Unified Communications Manager クラスタの試行されたコールと完了したコールを表す折れ線グラフを示しています。

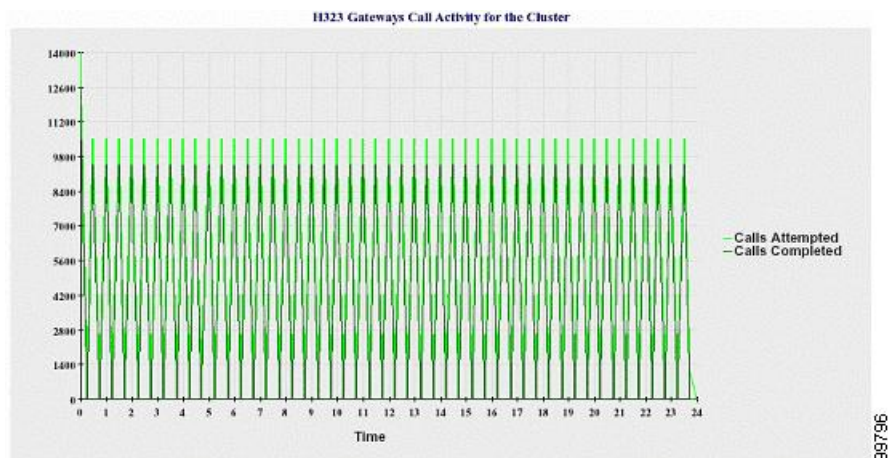


クラスタの H.323 ゲートウェイ コール アクティビティ

折れ線グラフには、H.323 ゲートウェイの試行されたコールと完了したコールの数が表示されます。Unified Communications Manager のクラスタ構成では、折れ線グラフはクラスタ全体の試行されたコールと完了したコールの数を表します。グラフは2本の線で構成されます。1本は試行されたコールの数、もう1本は完了したコールの数を示します。Unified Communications Manager のクラスタ構成では、各線はクラスタ値を表します。これは（データが利用できる）クラスタ内のすべてのサーバの値の合計と等しくなります。グラフ内の各データ値は、15分間に試行されたコールと完了したコールの総数を表します。完了したH.323ゲートウェイコールのデータが存在しない場合、完了したコールのデータを表す線は生成されません。試行されたH.323ゲートウェイコールのデータが存在しない場合、試行されたコールのデータを表す線は生成されません。Unified Communications Manager のクラスタ構成では、クラスタ内のサーバのデータがない場合、Reporter はそのサーバで試行されたコールまたは完了したコールを表す線を生成しません。H.323ゲートウェイコールアクティビティのデータがまったく存在しない場合、グラフは生成されません。

図 16: クラスタの H.323 ゲートウェイ コール アクティビティを示す折れ線グラフ

次の図は、Unified Communications Manager クラスタの H.323 ゲートウェイ コール アクティビティを表す折れ線グラフを示しています。

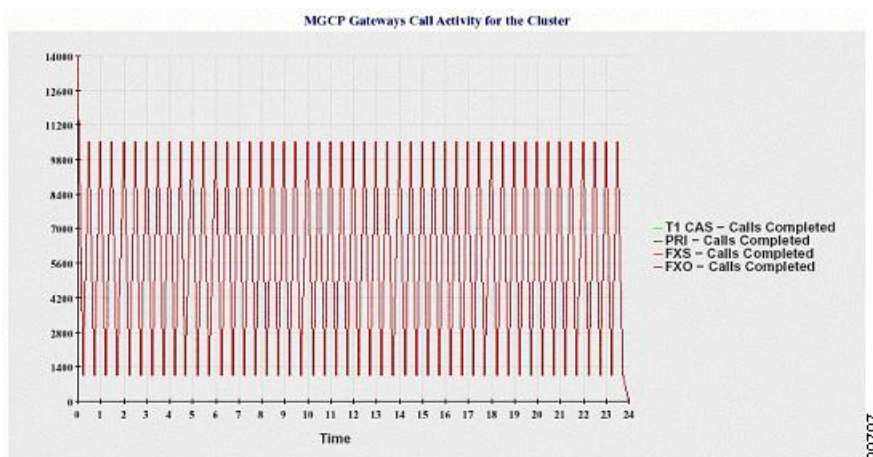


クラスタの MGCP ゲートウェイ コール アクティビティ

折れ線グラフには、TICAS ゲートウェイに対して1時間に完了したコールの数が表示されます。Unified Communications Manager クラスタ構成では、グラフには Unified Communications Manager クラスタ全体の完了したコールの数が表示されます。グラフは最大 4 本の線で構成され、完了したコールの数が（データが利用できる）ゲートウェイタイプごとに示されます。グラフ内の各データ値は、15分の間に完了したコールの総数を表します。ゲートウェイのデータが存在しない場合、Reporter は特定のゲートウェイに対して完了したコールのデータを表す行を生成しません。すべてのゲートウェイに関してデータが存在しない場合、グラフは生成されません。

図 17: クラスタの MGCP ゲートウェイ コール アクティビティを示す折れ線グラフ

次の図は、Unified Communications Manager クラスタの MGCP ゲートウェイ コール アクティビティを表す折れ線グラフを示しています。

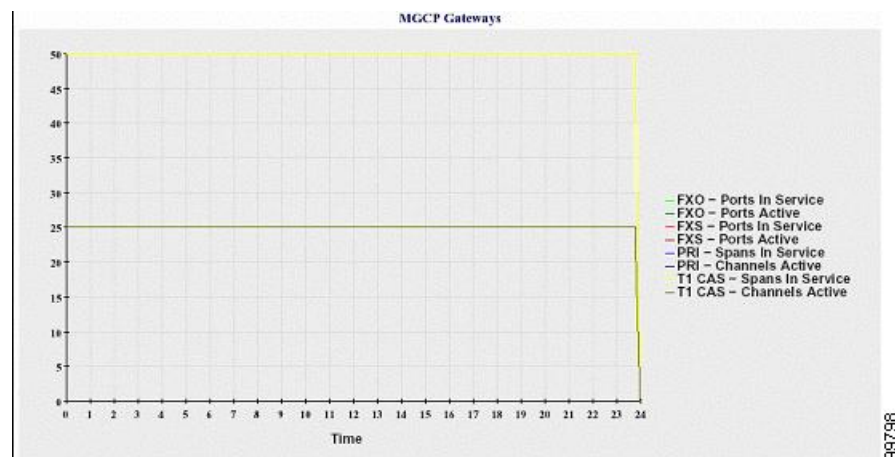


MGCP ゲートウェイ

折れ線グラフには、MGCP FXO ゲートウェイと FXS ゲートウェイの稼働中のポートおよびアクティブポートの数、および PRI ゲートウェイと TICAS ゲートウェイの稼働中のスパンまたはアクティブチャンネルの数が表示されます。Unified Communications Manager クラスタ構成の場合、グラフには Unified Communications Manager クラスタ全体のデータが表示されます。このチャートは、8つの回線で構成されており、それぞれが1つのサービスを提供しているポートの数については、各回線に2つの回線があります。サービス内の Span の数と、PRIおよびTICAS ゲートウェイに対してアクティブなチャンネルには、さらに4つの行があります。Unified Communications Manager のクラスタ構成では、各線はクラスタ値を表します。これは（データが利用できる）クラスタ内のすべてのサーバの値の合計です。グラフ内の各データ値は、15分間での稼働中のポートの総数、アクティブポートの数、稼働中のスパンの数、またはアクティブチャンネルの数を表します。サービス内の Span の数、またはすべてのサーバのゲートウェイに対してアクティブなチャンネル (TICAS) のデータが存在しない場合、Reporter はその特定のゲートウェイのデータを表す行を生成しません。

図 18: MGCP ゲートウェイを示す折れ線グラフ

次の図は、[参照 (the)] の CP ゲートウェイを表す折れ線グラフを示しています。

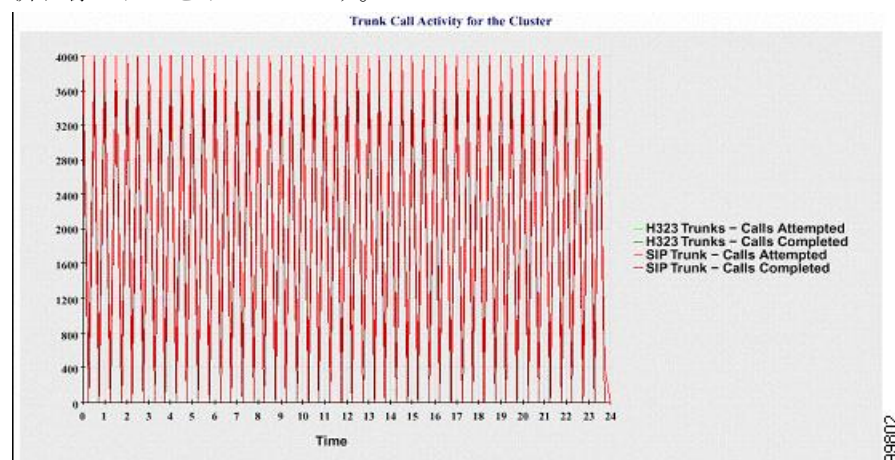


クラスタのトランク コール アクティビティ

折れ線グラフには、SIP トランクと H.323 トランクの1時間に完了したコールと試行されたコールの数が表示されます。Unified Communications Manager クラスタ構成の場合、グラフには Unified Communications Manager クラスタ全体の完了したコールと試行されたコールの数が表示されます。グラフは4本の線で構成されます。2本は（データが利用できる）各 SIP および H.323 トランクの完了したコールの数、もう2本は試行されたコールの数を示します。Unified Communications Manager のクラスタ構成では、各線はクラスタ値を表します。これは（データが利用できる）クラスタ内のすべてのノードの値の合計です。グラフ内の各データ値は、15分の間に完了したコールの総数または試行されたコールの数を表します。トランクのデータが存在しない場合、その特定のトランクについて完了したコールまたは試行されたコールを表す線は生成されません。両方のトランクタイプに関してデータが存在しない場合、グラフは生成されません。

図 19: クラスタのトランク コール アクティビティを示す折れ線グラフ

下の図は、Unified Communications Manager クラスタのトランク コール アクティビティを表す折れ線グラフを示しています。



サーバ（または Unified Communications Manager クラスタ構成内の各サーバ）には、ファイル名パターン CallLog_mm_dd_yyyy_hh_mm.csv に一致するログファイルが格納されています。ログファイルには次の情報が格納されています。

- Unified Communications Manager（または Unified Communications Manager クラスタ内の各サーバ）の試行されたコールおよび完了したコール
- H.323 ゲートウェイ（または Unified Communications Manager クラスタ内の各サーバのゲートウェイ）の試行されたコールおよび完了したコール
- MGCP FXO、FXS、PRI、T1CAS ゲートウェイ（または Unified Communications Manager クラスタ内の各サーバのゲートウェイ）の完了したコール
- （Unified Communications Manager クラスタ内の各サーバの）MGCP FXO ゲートウェイと FXS ゲートウェイの稼働中のポートおよびアクティブポート、および PRI ゲートウェイと T1CAS ゲートウェイの稼働中のスパンおよびアクティブチャンネル
- H.323 トランクと SIP トランクの試行されたコールおよび完了したコール

アラート要約レポート

アラート サマリー レポートには、その日に生成されたアラートの詳細が表示されます。

クラスタ固有の統計情報は、Unified Communications Manager および IM and Presence Service でのみサポートされます。

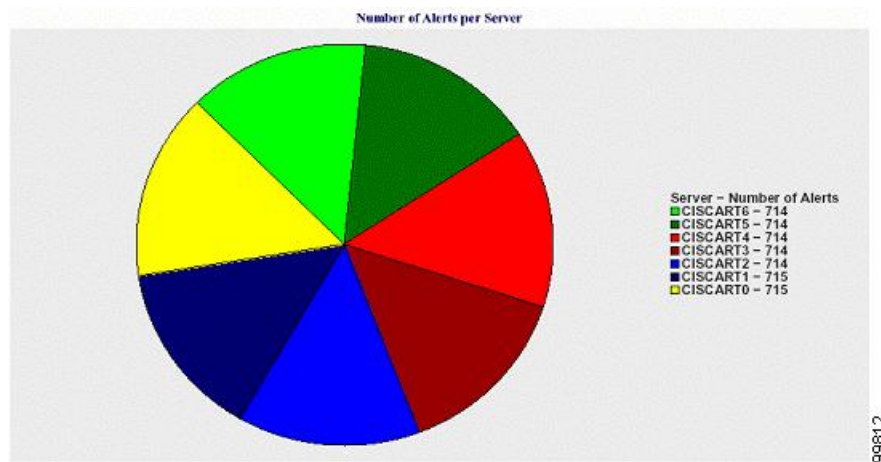
サーバごとのアラートの数

円グラフには、クラスタ内のノードごとのアラート数が表示されます。グラフには、生成されたアラートのサーバ全体の詳細が表示されます。円グラフの各領域は、クラスタの特定のサーバに対して生成されたアラートの数を表しています。グラフには、クラスタ内のサーバ（Reporter によってその日にアラートが生成されたサーバ）と同じ数の領域が含まれます。あるサーバのデータがない場合、そのサーバを表すチャートの領域はありません。すべてのサーバのデータが存在しない場合はグラフが生成されません。「指定された日に生成されたアラートはありません」というメッセージが表示されます。

Cisco Unity Connectionのみ:円グラフには、サーバのアラート数が表示されます。グラフには、生成されたアラートのサーバ全体の詳細が表示されます。サーバのデータが存在しない場合はグラフが生成されません。メッセージ「その日はアラートが生成されませんでした（No alerts were generated for the day）」が表示されます。

下のグラフは、Unified Communications Manager クラスタ内のサーバごとのアラートの数を表す円グラフの例を示します。

図 20: サーバごとのアラート数を示す円グラフ

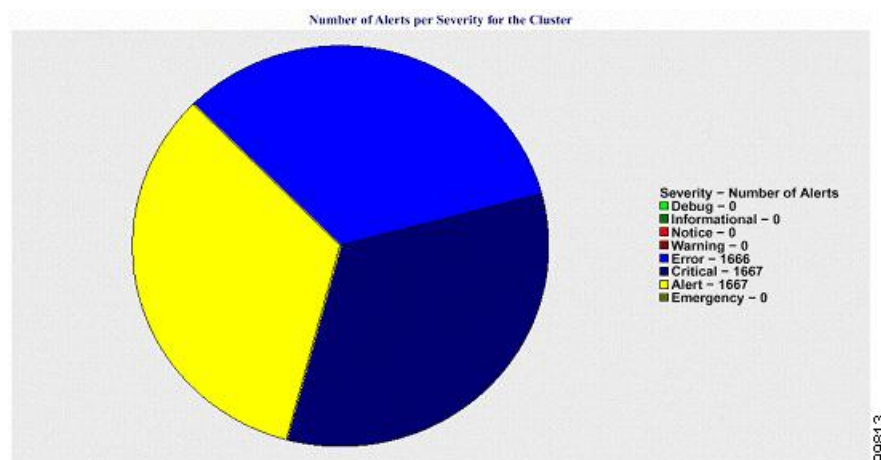


クラスタのシビラティ（重大度）ごとのアラート数

アラートのシビラティ（重大度）ごとのアラート数が円グラフに表示されます。グラフには、生成されたアラートのシビラティ（重大度）の詳細が表示されます。円グラフの各領域は、生成された特定のシビラティ（重大度）タイプのアラートの数を表します。グラフには、（Reporterによってその日に生成されたアラートの）シビラティ（重大度）と同じ数の領域が含まれます。あるシビラティ（重大度）のデータがない場合、そのシビラティ（重大度）を表すチャートの領域はありません。データが存在しない場合はグラフが生成されません。

下のグラフは、Unified Communications Manager クラスタのシビラティ（重大度）ごとのアラートの数を表す円グラフの例を示します。

図 21: クラスタのシビラティ（重大度）ごとのアラート数を示す円グラフ



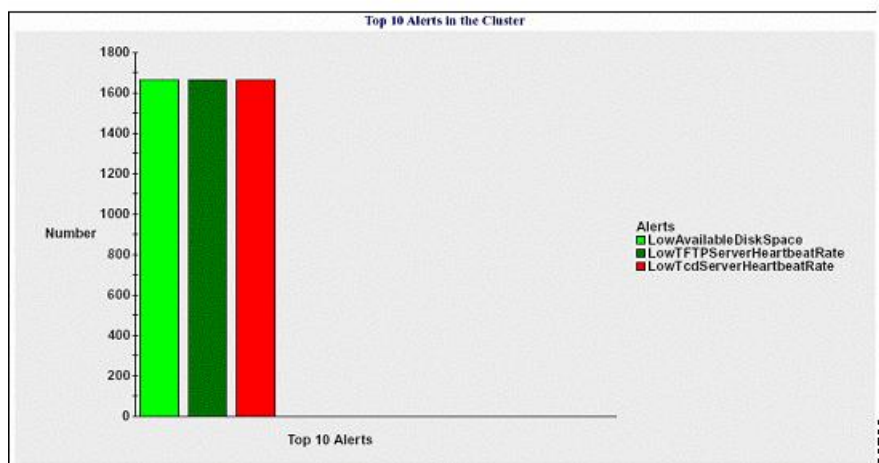
クラスタ内の上位 10 のアラート

特定のアラートタイプのアラート数が棒グラフに表示されます。グラフには、アラートタイプに基づいて生成されたアラートの詳細が表示されます。それぞれの折れ線は、そのアラート

タイプのアラートの数を表します。グラフには、アラート数が多いものから順に、最初の 10 個のアラートの詳細のみが表示されます。特定のアラートタイプのデータがない場合、そのアラートを表す折れ線はありません。アラートタイプのデータがない場合はグラフが生成されません。

下のグラフは、Unified Communications Manager クラスタ内の上位 10 のアラートを表す棒グラフの例を示しています。

図 22: クラスタ内の上位 10 のアラートを表す棒グラフ



サーバ（またはクラスタ内の各サーバ）には、ファイル名パターン `AlertLog_mm_dd_yyyy_hh_mm.csv` に一致するログファイルが格納されています。ログファイルには次の情報が格納されています。

- 時刻：アラートが発生した時刻
- アラート名-説明的な名前
- ノード名：アラートが発生したサーバ
- モニタ対象オブジェクト：モニタされるオブジェクト
- シビラティ（重大度）：アラートのシビラティ（重大度）

パフォーマンス保護レポート

パフォーマンス保護レポートでは、IM and Presence サービスと Cisco Unity Connection はサポートされていません。

パフォーマンス保護レポートには、特定のレポートの統計情報を表示するさまざまなグラフで構成される要約が表示されます。Reporter は、ログに記録された情報に基づいてレポートを 1 日 1 回生成します。

パフォーマンス保護レポートは、過去7のデフォルトのモニタリングオブジェクトに関するトレンド分析情報を提供します。これにより、シスコの会社間メディアエンジンに関する情報を

追跡できます。このレポートには、cisco ime クライアントの合計コール数とフォールバックコール比率を示すCisco Imeクライアントコールアクティビティチャートが含まれています。

パフォーマンス保護レポートは、次のグラフで構成されます。

- Cisco Unified Communications Manager コール アクティビティ
- 登録済み電話機および MGCP ゲートウェイの数
- システム リソースの使用率 (System Resource Utilization)
- デバイスとダイヤル プランの数量

Cisco Unified Communications Manager コール アクティビティ

折れ線グラフには、試行されたコールと完了したコールの数の1時間ごとの増減率がアクティブ コール数として表示されます。Unified Communications Manager のクラスタ構成では、クラスタ内の各サーバのデータのグラフが作成されます。グラフは3本の線で構成され、それぞれ試行されたコールの数、完了したコールの数、およびアクティブ コールを示します。コールアクティビティのデータが存在しない場合、Reporter はグラフを生成しません。

登録済み電話機および MGCP ゲートウェイの数

折れ線グラフには、登録済み電話機および MGCP ゲートウェイの数が表示されます。Unified Communications Manager のクラスタ構成の場合、グラフにはクラスタ内の各サーバのデータが表示されます。グラフは2本の線で構成され、1本は登録済み電話機の数、もう1本はMGCPゲートウェイの数を示します。電話機またはMGCPゲートウェイのデータがない場合、Reporter はグラフを生成しません。

システム リソースの使用率 (System Resource Utilization)

折れ線グラフには、サーバ（または Unified Communications Manager クラスタ構成のクラスタ全体）の CPU 負荷率とメモリ使用率（バイト）が表示されます。グラフは2本の線で構成され、1本はCPU負荷、もう1本はメモリ使用率を示します。Unified Communications Manager のクラスタでは、各線はクラスタ値を表します。これは（データが利用できる）クラスタ内のすべてのサーバの値の平均です。電話機またはMGCPゲートウェイのデータがない場合、Reporter はグラフを生成しません。

デバイスとダイヤル プランの数量

2つのテーブルに、デバイスの数およびダイヤル プラン コンポーネントの数に関する Unified Communications Manager データベースの情報が表示されます。デバイステーブルは、IP 電話、Cisco Unity Connection ポート、H.323 クライアント、H.323 ゲートウェイ、MGCP ゲートウェイ、MOH リソース、およびMTPリソースの数を示します。ダイヤルプランテーブルは、ディレクトリ番号と回線、ルートパターン、およびトランスレーションパターンの数を示します。



第 22 章

Cisco Unified Reporting

- 統合されたデータのレポート (351 ページ)
- システム要件 (352 ページ)
- UI のコンポーネント (353 ページ)
- サポートされているレポート (355 ページ)

統合されたデータのレポート

Cisco Unified Communications Manager および Cisco Unified Communications Manager IM and Presence Service コンソールからアクセスする Cisco Unified Reporting Web アプリケーションは、トラブルシューティングまたはクラスタ データの調査のための統合レポートを生成します。



(注) 特に指定のない限り、このマニュアルの情報、注記、手順は Unified Communications Manager と IM and Presence Service に適用されます。

このツールは、クラスタデータのスナップショットを簡単に作成する方法を提供します。このツールは、既存のソースからのデータの収集、データの比較、および異常の報告を行います。Cisco Unified Reporting でレポートを生成すると、レポートでは、1 台以上のサーバにある 1 つ以上のソースからのデータを結合して、1 つの出力ビューを作成します。たとえば、クラスタ内の全サーバの *hosts* ファイルを表示するレポートを参照できます。

Cisco Unified Reporting Web アプリケーションは、インストール時にクラスタ内のすべてのサーバに展開されます。レポートは、データベース レコードから生成されます。

レポートの生成に使用するデータ ソース

このアプリケーションでは、パブリッシャ サーバと各サブスクライバサーバに格納されている次のいずれかのソースから情報を取り込みます。

- RTMT カウンタ
- CDR_CAR (Unified Communications Managerのみ)

- Unified Communications ManagerDB (Unified Communications Managerのみ)
- IM and Presence DB (IM and Presenceのみ)
- ディスク ファイル
- OS API 呼び出し
- ネットワーク API 呼び出し
- prefs
- CLI
- RIS

レポートには、レポートの生成時点でアクセスできるすべてのアクティブなクラスタノードのデータが取り込まれます。パブリッシャ サーバのデータベースが停止している場合は、アクティブなノードのレポートを生成できます。System Reports リストにある Report Descriptions レポートは、レポートの情報ソースを提供します。

サポートされている出力形式

このリリースでは、レポートのHTML/CSV出力をサポートしています。Cisco Unified Reporting では、レポート名と日付と時刻のスタンプによってレポートを識別できます。このアプリケーションでは、ユーザが表示できるように最近のレポートのローカル コピーが保管されます。「新しいレポートのダウンロード」で説明しているように、最近のレポートのローカル コピーまたは新しいレポートをハードディスクにダウンロードすることができます。レポートをダウンロードするときは、区別するためにダウンロードするファイルの名前を変更するか、別のフォルダに保存できます。

システム要件

Cisco Tomcat Service

Cisco Unified Reporting は、Cisco Tomcat サービス上でアプリケーションとして実行されます。このアプリケーションはUnified Communications Manager、および IM and Presence Serviceのインストール時にアクティブ化されます。これらの製品がクラスタ内のすべてのサーバで稼働していることを確認します。

HTTPS

レポート サブシステムでは、HTTPS 経由で RPC メカニズムを使用して他のサーバから情報を収集します。レポートが正常に生成されるように、サーバでHTTPS ポートが開いていて、Cisco Tomcat サービスを実行していることを確認します。

HTTPS を有効にするには、接続プロセス中にサーバ識別用の証明書をダウンロードする必要があります。現在のセッションだけにサーバ証明書を使用するか、サーバでの現在のセッション

ンと将来のセッションのセキュリティを確保するために信頼フォルダ（ファイル）に証明書をダウンロードすることができます。信頼フォルダには、すべての信頼済みサイトの証明書を保存します。HTTPSの詳細については、『*Cisco Unified Communications Manager Administration Guide*』の「Introduction」の章を参照してください。

アプリケーションにアクセスするには、ブラウザウィンドウの管理インターフェイスにアクセスします。Cisco Unified Reporting では、HTTPS を使用してブラウザとのセキュアな接続を確立します。

必要なアクセス権限

Cisco Unified Reporting アプリケーションでは、Cisco Tomcat サービスを使用してユーザを認証してから、Web アプリケーションへのアクセスを許可します。権限のあるユーザだけが Cisco Unified Reporting アプリケーションにアクセスできます。Unified Communications Manager の場合、デフォルトでは、Standard CCM Super Users グループの管理者ユーザだけが Cisco Unified Reporting にアクセスして、レポートを表示、作成できます。

Cisco Unified Communications Manager および IM and Presence Service の場合は、Standard CUReporting 認証ロールのユーザが Cisco Unified Reporting にアクセスできます。

権限のあるユーザは、Cisco Unified Reporting ユーザ インターフェイスを使用して、レポートの表示、新しいレポートの生成、およびレポートのダウンロードを実行できます。

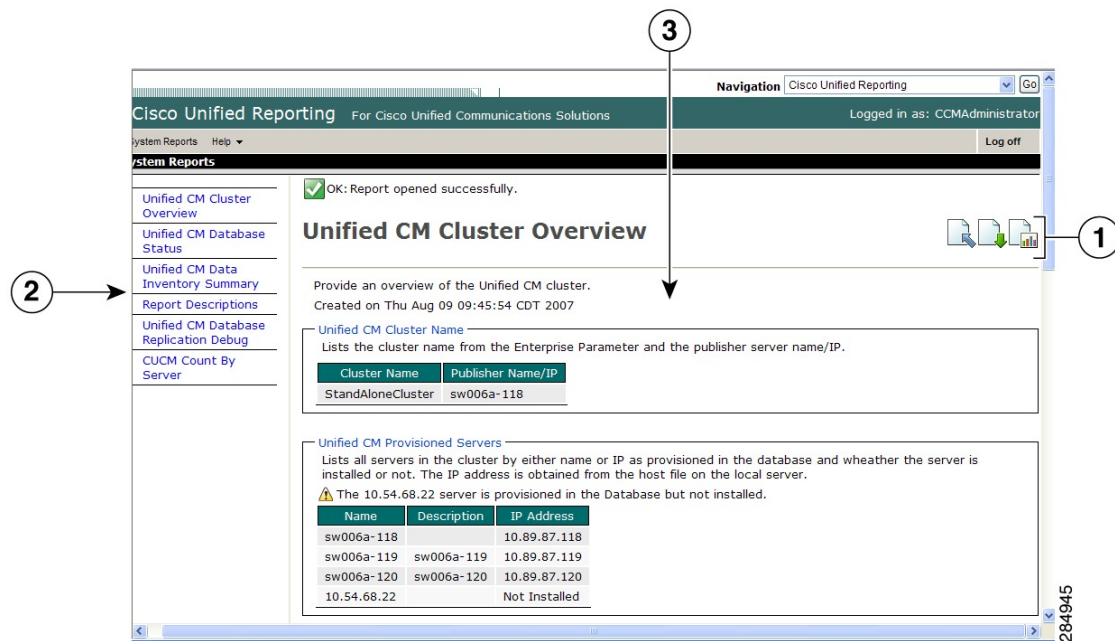


-
- (注) に Unified Communications Manager、Standard CCM Super Users グループの管理者ユーザはアプリケーションの 1 個に管理の Unified Communications Manager ナビゲーションメニューの管理アプリケーションに、SSO を備えた Cisco Unified Reporting など、アクセスできます。
-

UI のコンポーネント

次の図に、Cisco Unified Reporting の UI のコンポーネントを示します。

図 23: UI のコンポーネント



1. [アップロード (Upload)]、[ダウンロード (Download)]、[生成 (Generate)]アイコン
2. レポート リスト
3. レポートの詳細



(注) レポートのカテゴリ、使用できるレポート、およびレポートのデータは、リリースによって異なります。

管理インターフェイスからのログイン

次のいずれかの手順を実行し、管理インターフェイスから Cisco Unified Reporting にログインします。

- に Unified Communications Manager、Cisco Unified CM Administration インターフェイスのナビゲーションメニューから **[Cisco Unified Reporting]** を選択します。
- IM and Presence Service の場合は、IM and Presence 管理インターフェイスのナビゲーションメニューから **[Cisco Unified IM and Presence Reporting]** を選択します。

始める前に

Cisco Unified Reporting アプリケーションへのアクセスが許可されていることを確認します。

シスコのユニファイドレポートにログインすると、最後に成功したシステムログイン試行と、ユーザ id、日付、時刻、および IP アドレスとともに、各ユーザに対する最後の失敗したシステムログイン試行が、メインのシスコユニファイドレポートウィンドウに表示されます。

サポートされているレポート

このセクションでは、Cisco Unified Communications Manager および Cisco Unified Communications Manager IM and Presence Service でサポートされているレポートの詳細について説明します。Cisco Unified Reporting では、レポート名と日付と時刻のスタンプによってレポートを識別できます。Cisco Unified Reporting では、ユーザが表示できるように最近のレポートのローカルコピーが保管されます。

Unified Communications Manager レポート

次の表に、Unified Communications Manager をインストールした後に Cisco Unified Reporting に表示されるシステム レポートの種類を示します。

表 75: *Unified Communications Manager Cisco Unified Reporting* で表示されるレポート

レポート	説明
期限切れのクレデンシャルアルゴリズムを使用したユーザの UCM	では、SHA1 を使用してパスワードまたは Pin が保存され、ハッシュされているエンドユーザのリストを提供しています。
Report Descriptions	表示しているレポートに関するトラブルシューティング情報と詳細情報を提供します。
セキュリティ診断ツール (Security Diagnostic Tool)	セキュリティ コンポーネントに関する情報の要約を提供します。
Unified CM クラスタの概要 (Unified CM Cluster Overview)	Unified Communications Manager クラスタの概要を提供します。このレポートには、次の詳細情報が含まれています。 <ul style="list-style-type: none"> Unified Communications Manager または IM and Presence クラスタにインストールしたバージョンを保守します。 クラスタ内のすべてのサーバのホスト名または IP アドレス ハードウェア詳細情報の要約

レポート	説明
Unified CM データ サマリ (Unified CM Data Summary)	データベースUnified Communications Managerにある場合にUnified Communications Managerメニュー構造に従ってデータの要約が示されます。たとえば、3つのクレデンシャルポリシー、5つの会議ブリッジ、10のシェアドラインアピランスを設定した場合、このレポートに含まれる情報のタイプを確認できます。
Unified CM データベース複製のデバッグ (Unified CM Database Replication Debug)	データベース複製のためのデバッグ情報を提供します。 ヒント このレポートを生成すると、CPUの使用率が急増し、生成するのにクラスタ内のサーバごとに最大10秒かかる可能性があります。
Unified CM データベース ステータス (Unified CM Database Status)	Unified Communications Manager データベースのヘルス スナップショットを提供します。アップグレードする前にこのレポートを生成して、データベースが正常であることを確認します。
Unified CM デバイス カウント サマリ (Unified CM Device Counts Summary)	存在Unified Communications Managerするデバイスの数を、モデルおよびプロトコル別に示します。
Unified CM デバイス 配信 サマリ (Unified CM Device Distribution Summary)	クラスタに分散されたデバイスの要約を提供します。たとえば、このレポートは、プライマリ ノード、セカンダリ ノード、ターシャリ ノードなどに関連付けられているデバイスを示します。
Unified CM ディレクトリ URI および GDPR 重複 (Unified CM Directory URI and GDPR Duplicates)	システムで重複ユーザディレクトリ URI、学習された Directories URI、学習された数と学習されたパターンの詳細が記載されています。
Unified CM Extension Mobility	Cisco Extension Mobility の使用状況の要約を提供します。たとえば、Cisco Extension Mobility ユーザがログインしている電話機の数、Cisco Extension Mobility に関連付けられたユーザなどです。
Unified CM GeoLocation ポリシー (Unified CM GeoLocation Policy)	GeoLocation 論理パーティションポリシーマトリクスのレコードの一覧を提供します。
Unified CM GeoLocation ポリシーとフィルタ (Unified CM GeoLocation Policy with Filter)	選択した GeoLocation ポリシーに対する、GeoLocation 論理パーティション ポリシー マトリクス のレコード の一覧 を提供 します。

レポート	説明
電話機に関連付けられていない Unified CM 回線 (Unified CM Lines Without Phones)	電話機に関連付けられていない回線の一覧を提供します。
Unified CM 複数回線デバイス (Unified CM Multi-Line Devices)	複数ライン アピランスを使用する電話機の一覧を提供します。
Unified CM 電話機カテゴリ (Unified CM Phone Category)	ユニバーサル デバイス テンプレートを使用して特定のカテゴリの電話機モデルの一覧を示します。社員のセルフプロビジョニングを有効にすると、各カテゴリのテンプレートを提供することによって、電話機のこれらのカテゴリのいずれか、またはすべてを許可することを選択できます。
Unified CM 電話機能リスト (Unified CM Phone Feature List)	Unified Communications Manager のデバイス タイプごとにサポートされる機能の一覧を提供します。
Unified CM 電話機ロケール インストーラ (Unified CM Phone Locale Installers)	インストールされている電話ロケール パッケージでサポートされる Cisco Unified IP Phone ファームウェアバージョンのリストを提供します。
ロードに不整合が発生した Unified CM 電話機 (Unified CM Phones With Mismatched Load)	ファームウェア ロードに不整合が発生したすべての電話機の一覧を提供します。
回線が関連付けられていない Unified CM 電話機 (Unified CM Phones Without Lines)	Unified Communications Manager データベース内の、関連付けられた回線を持たないすべての電話機の一覧を提供します。
Unified CM シェア ドライン (Unified CM Shared Lines)	Unified Communications Manager データベース内の、少なくとも 1 つのシェア ドライン アピランスを使用しているすべての電話機の一覧を提供します。
Unified CM テーブル カウント サマリ (Unified CM Table Count Summary)	データベースを中心にデータを表示します。このレポートは、データベース スキーマを理解している管理者または AXL API 開発者の役に立ちます。
Unified CM ユーザ デバイス カウント (Unified CM User Device Count)	関連するデバイスに関する情報を提供します。たとえば、このレポートは、ユーザのいない電話機の数、1 つの電話機を持つユーザの数、複数の電話機を持つユーザの数を一覧表示します。
プライマリ内線番号を共有している Unified CM ユーザ (Unified CM Users Sharing Primary Extensions)	システムのプライマリ内線番号を共有するユーザのリストを提供します。

レポート	説明
Unified CM VG2XX ゲートウェイ (Unified CM VG2XX Gateway)	ゲートウェイ エンドポイントのセキュリティプロファイルの概要を示します。
Unified CM ボイスメール (Unified CM Voice Mail)	Unified Communications Manager Administration のボイスメッセージング関連の設定の要約を提供します。たとえば、このレポートは、設定されたボイスメール ポートの数、メッセージ待機インジケータの数、設定されたボイスメッセージプロファイルの数、ボイスメッセージプロファイルに関連付けられたディレクトリ番号の数、などを示します。
Unified 内部アクセス レベルマトリックス (Unified Confidential Access Level Matrix)	内部アクセス レベル マトリックスに関するすべての情報が提供されます。

IM and Presence Service レポート

次の表に、Unified Communications Manager で IM and Presence Service をインストールした後に Cisco Unified Reporting に表示されるシステム レポートの種類を示します。



- (注) リリース 10.0(1) から、IM and Presence クラスタの情報は、Cisco Unified Communications Manager ノードから入手できます。Cisco Unified Communications Manager から、**Cisco ユニファイドレポート** > システムレポート > **Unified CM クラスタの概要** を選択します。

次の表にあるレポートの種類を表示および生成できます。

表 76: Cisco Unified Reporting に表示される IM and Presence Service レポート

レポート	説明
IM and Presence データベース複製のデバッグ (IM and Presence Database Replication Debug)	データベース複製のためのデバッグ情報を提供します。 ヒント このレポートを生成すると、CPU の使用率が急増し、生成するのにクラスタ内のサーバごとに最大 10 秒かかる可能性があります。
IM and Presence データベースステータス (IM and Presence Database Status)	IM and Presence Service データベースのヘルス スナップショットを提供します。アップグレードする前にこのレポートを生成して、データベースが正常であることを確認します。
IM and Presence テーブル カウント サマリ (IM and Presence Table Count Summary)	データベースを中心にデータを表示します。このレポートは、データベース スキーマを理解している管理者または AXL API 開発者の役に立ちます。

レポート	説明
IM and Presence ユーザセッションレポート	1つ以上のデバイスとのすべてのアクティブユーザサインインセッションのリストが表示されます。
プレゼンス設定レポート (Presence Configuration Report)	<p>IM and Presence Service ユーザに関する設定情報を提供します。</p> <ul style="list-style-type: none"> • Cisco Unified Communications Manager から同期されたユーザ • IM and Presence Serviceが有効なユーザ • Microsoft リモート通話コントロールが有効なユーザ • IM and Presence Serviceの予定表情報が有効なユーザ <p>ソート可能なカラムのユーザのリストを表示するには、[詳細表示 (View Details)]をクリックします。</p>
IM and Presence クラスタの概要 (IM and Presence Cluster Overview)	IM and Presence Service クラスタの概要を提供します。このレポートでは、クラスタにインストールされている IM and Presence Serviceのバージョン、クラスタ内のすべてのサーバのホスト名または IP アドレス、ハードウェア詳細情報の要約などを確認できます。
Presence Limits Warning Report	<p>接続またはウォッチャの設定の制限値の最大数を満たしているか、超えてしまったユーザに関する情報を提供します。</p> <p>ソート可能なカラムのユーザのリストを表示するには、[詳細表示 (View Details)]をクリックします。</p>
プレゼンス使用レポート (Presence Usage Report)	<p>ログインした XMPP クライアントとサードパーティ API の使用情報を提供します。</p> <p>ソート可能なカラムの XMPP クライアントとサードパーティ API のリストを表示するには、[詳細表示 (View Details)]をクリックします。</p>
レポートの説明 (Report Descriptions)	表示しているレポートに関するトラブルシューティング情報と詳細情報を提供します。このレポートでは、レポート、各情報グループ、各データ項目、データソース、関連する問題の現象、および対処方法を説明します。

レポートの説明の表示

Cisco Unified Reporting では、レポートのヘルプが用意されています。[レポートの説明 (Report Descriptions)]リンクでは、レポート、各情報グループ、各データ項目、データソース、関連する問題の現象、および対処方法を説明します。



(注) その他のレポートの問題については、TAC にお問い合わせください。

手順

ステップ 1 [システム レポート (System Reports)] を選択します。

ステップ 2 レポートのリストで [レポートの説明 (Report Descriptions)] リンクを選択します。

(注) IM and Presence Service レポートを選択したときに再ログインを要求された場合は、Cisco Unified Communications Manager の管理者ログインクレデンシャルを再入力します。

ステップ 3 [レポートの生成 (Generate Report)] アイコンを選択します。

レポートが生成され、表示されます。

新規レポートの作成

新しいレポートを生成して、表示できます。

始める前に

1 台以上のサーバで Cisco Tomcat サービスが実行されていて、レポートの表示に関してサポートされている Web ブラウザを使用していることを確認します。

レポートを生成するのに非常に時間がかかる場合、または CPU 時間が非常に多くなる場合は、アプリケーションによって通知されます。レポートの生成中は経過表示バーが表示されます。新しいレポートが表示され、日付と時刻が更新されます。

手順

ステップ 1 メニューバーから [システム レポート (System Reports)] を選択します。

ステップ 2 いずれかのレポートを選択します。

(注) IM and Presence Service レポートを選択したときに再ログインを要求された場合は、Cisco Unified Communications Manager Administration のログインクレデンシャルを再入力します。

ステップ 3 [レポート (Reports)] ウィンドウで [レポートの生成 (Generate Report)] (棒グラフ) アイコンを選択します。

ステップ 4 [詳細の表示 (View Details)]リンクを選択して、自動的に表示されないセクションの詳細情報を表示します。

次のタスク

レポートで、項目に対するデータ チェックが失敗したことが示された場合は、[レポートの説明 (Report Descriptions)]レポートを選択して、トラブルシューティング情報と対処方法を確認します。レポートの説明レポートはデータベースから動的に生成されるので、新たに、新規のレポートの説明レポートを生成することもできます。

保存済みレポートの表示

既存のレポートのコピーを表示できます。



(注) Cisco Unified Reporting アプリケーションでは、フレッシュ インストールまたはアップグレード時に最近のレポートのローカル コピーが保存されません。

始める前に

1 台以上のサーバで Cisco Tomcat サービスが実行されていて、レポートの表示に関してサポートされている Web ブラウザを使用していることを確認します。

手順

ステップ 1 メニュー バーから [システム レポート (System Reports)]を選択します。

ステップ 2 レポート リストから表示するレポートを選択します。

ステップ 3 レポート名のリンクを選択します (日付と時刻が記録されています)。

ステップ 4 [詳細の表示 (View Details)]リンクを選択して、自動的に表示されないセクションの詳細情報を表示します。

次のタスク

新しいレポートまたは保存済みレポートをダウンロードします。

レポートで、項目に対するデータ チェックが失敗したことが示された場合は、[レポートの説明 (Report Descriptions)]レポートを選択して、対処方法に関するトラブルシューティング情報を確認します。

新しいレポートのダウンロード

新しいレポートをダウンロードする場合、レポートはローカルハードドライブに保存されます。レポートをダウンロードすると、raw XML データ ファイルがハードドライブにダウンロードされます。

手順

ステップ 1 新しいレポートを生成します。

ステップ 2 新しいレポートが表示されたら、[レポート (Reports)] ウィンドウで [レポートのダウンロード (Download Report)] (緑色の矢印) アイコンを選択します。

(注) ドキュメントをダウンロードする前に、[詳細の表示 (View Details)] リンクをクリックしてレポートの詳細情報を表示する必要はありません。データは、ダウンロードしたファイルで検出されます。

ステップ 3 [保存 (Save)] を選択して、指定したディスク上の場所にファイルを保存します。

ファイル名またはハードディスク上のファイルの保存場所を変更するには、新しい場所を入力するか、ファイルの名前を変更します (任意)。ダウンロード中は経過表示バーが表示されます。

ハードディスクにファイルがダウンロードされます。

ステップ 4 ダウンロードが完了したら、[開く (Open)] を選択して XML レポートを開きます。

(注) XML ファイルの内容を変更しない場合、レポートは画面で正しく表示されない場合があります。

次のタスク

ダウンロードされたレポートファイルをブラウザで表示するには、ファイルをサーバにアップロードします。



(注) テクニカルサポートを受けるときに、ダウンロードしたファイルを電子メールに添付するか、ファイルを別のサーバにアップロードできます。

保存済みレポートのダウンロード

保存済みレポートをダウンロードする場合、ダウンロードされたレポートはローカルハードドライブに保存されます。レポートをダウンロードすると、raw XML データ ファイルがハードディスクにダウンロードされます。

手順

- ステップ 1** 既存のレポートの詳細情報を開いて、表示します。
- ステップ 2** [レポート (Reports)] ウィンドウで[レポートのダウンロード (Download Report)] (緑色の矢印) アイコンを選択します。
- ステップ 3** [保存 (Save)] を選択して、指定したディスク上の場所にファイルを保存します。
ファイル名またはハードディスク上のファイルの保存場所を変更するには、新しい場所を入力するか、ファイルの名前を変更します (任意)。ダウンロード中は経過表示バーが表示されません。
ハードディスクにファイルがダウンロードされます。
- ステップ 4** ダウンロードが完了したら、[開く (Open)] を選択して XML レポートを開きます。
(注) XML ファイルの内容を変更しない場合、レポートは正しく表示されない場合があります。

次のタスク

ダウンロードされたレポートファイルをブラウザで表示するには、ファイルをサーバにアップロードします。



- (注) テクニカルサポートを受けるときに、ダウンロードしたファイルを電子メールに添付するか、ファイルを別のサーバにアップロードできます。

レポートのアップロード

ダウンロードされたレポートをブラウザウィンドウで表示するには、レポートをサーバにアップロードする必要があります。

始める前に

ハードドライブにレポートをダウンロードします。

手順

- ステップ 1** メニューバーから [システム レポート (System Reports)] を選択します。
- ステップ 2** レポートにアクセスすると、[レポート (Reports)] ウィンドウに [レポートのアップロード (Upload Report)] アイコン (青色の矢印) が表示されます。
- ステップ 3** [レポートのアップロード (Upload Report)] アイコンを選択します。

- ステップ 4** .xml ファイルの場所を指定するには、[参照 (Browse)] を選択して、ハードドライブ上のファイルの場所に移動します。
- ステップ 5** [アップロード (Upload)] を選択します。
- ステップ 6** [続行 (Continue)] を選択して、アップロードしたファイルをブラウザ ウィンドウに表示します。
-

次のタスク

アップグレードするときにアップロードしたレポートと新しく生成したレポートを並べて比較できます。



第 23 章

Cisco IP Phone 電話の通話診断と品質レポートを設置する

- [診断およびレポートの概要 \(365 ページ\)](#)
- [前提条件 \(366 ページ\)](#)
- [Diagnostics and Reporting の設定タスク フロー \(368 ページ\)](#)

診断およびレポートの概要

Cisco Unified Communications Manager には、Cisco IP Phone の通話品質を保証するためのオプションが 2 つあります。

- コール診断: コールの診断には、コール管理レコード (CMR) と音声品質メトリックの生成が含まれています。
- 品質報告ツール QRT-QRT は Cisco Unified IP 電話の音声品質と一般的な問題報告ツールです。このツールを使用すると、ユーザは IP 電話に音声やその他の一般的な問題を簡単に、かつ正確にレポートできます。

コール診断の概要

コール診断を収集するために、SCCP と SIP を実行している Cisco IP Phone を設定することができます。通話診断には、診断記録とも呼ばれる通話管理記録 (CMR) と音声品質指標が含まれます。

音声品質メトリックは、デフォルトで有効になっており、ほとんどの Cisco IP Phone でサポートされています。Cisco IP Phone は、MOS (平均意見四つ角) 値に基づいて音声品質メトリックを計算します。音声品質メトリックでは、ノイズや歪みは考慮されません。フレーム損失だけが考慮されます。

CMR レコードには、コールの音声ストリームの品質に関する情報が格納されます。CMR を生成するように Unified Communications Manager を設定できます。この情報は、請求レコードの生成やネットワーク分析などの後処理活動に使用できます。

品質レポートツールの概要

品質レポートツール (QRT) は、Cisco IP 電話の音声品質と一般的な問題をレポートするツールです。このツールを使用すると、ユーザは IP 電話に音声やその他の一般的な問題を簡単に、かつ正確にレポートできます。

システム管理者は、ユーザの IP 電話に QRT ソフトキーを表示するソフトキーテンプレートを設定して割り当てることで、QRT 機能を有効化できます。QRT を使用して行うユーザインタラクションのレベルに応じて、2つの異なるユーザモードを選択できます。次に、システムにおける機能の動作を定義するため、システムパラメータを設定し、Cisco Unified Serviceability ツールを設定します。QRT Viewer アプリケーションを使用して、電話の問題レポートを作成、カスタマイズ、および表示できます。

ユーザの IP 電話で問題が発生した場合、ユーザは、コールの状態がオンフックまたは接続済みのときに Cisco IP 電話の QRT ソフトキーを押すことで、問題のタイプとその他の関連統計をレポートできます。ユーザは IP 電話で報告されている問題を最もよく表している理由コードを選択できます。カスタマイズされた電話の問題レポートには、具体的な情報が表示されます。

ユーザが QRT ソフトキーを押して問題の種類を選択すると、QRT はストリーミングの統計情報を収集しようとします。ストリーミングの統計情報を収集するには、QRT でコールを 5 秒以上アクティブにする必要があります。

詳細なコールレポートおよび課金情報

Cisco CDR Analysis and Reporting (CAR) ツールは、サービス品質、トラフィック、ユーザコール量、課金情報、ゲートウェイに関する詳細なレポートを生成します。CAR は、コール詳細レコード (CDR)、コール管理レコード (CMR)、および Unified Communications Manager データベースのデータを使用してレポートを生成します。CAR インターフェイスには、Cisco Unified Serviceability の [ツール (Tools)] メニューからアクセスできます。

CAR は、サードパーティが提供するコールアカウンティング/課金ソリューションに代わるものではありません。Cisco Developer Community のホームページで、これらのソリューションを提供する、Cisco Technology Developer Program のメンバ企業を検索できます。

CAR でレポートを設定する方法の詳細については、『Cisco Unified Communications Manager のコールレポートおよび課金管理ガイド』を参照してください。

前提条件

コール診断の要件

Cisco Unified IP Phone がコール診断をサポートしているかどうかを確認します。

次の表を使用して、電話機がコール診断をサポートしているかどうかを確認します。コール診断の凡例は、次のようにサポートされています。

- X : SCCP と SIP の両方を実行している電話機によるサポート
- S : SCCP 機能のみ

表 77: コール診断のデバイスサポート

デバイス	コール診断のサポート
Cisco Unified IP Phone 7906	X
Cisco Unified IP Phone 7911	X
Cisco Unified IP Phone 7931	X
Cisco Unified IP Phone 7940	S
Cisco Unified IP Phone 7941	X
Cisco Unified IP Phone 7942-G	X
Cisco Unified IP Phone 7942-G/GE	X
Cisco Unified IP Phone 7945	X
Cisco Unified IP Phone 7960	S
Cisco Unified IP Phone 7961	X
Cisco Unified IP Phone 7962-G	X
Cisco Unified IP Phone 7962-G/GE	X
Cisco Unified IP Phone 7965	X
Cisco Unified IP Phone 7972-G/GE	X
Cisco Unified IP Phone 7975	X

品質レポートツールの要件

Cisco IP電話の機能：

- ソフトキー テンプレートのサポート
- IP Phone サービスのサポート
- CTI による制御が可能
- 内部 HTTP サーバを含む

詳細については、お使いの電話モデルのガイドを参照してください。

Diagnostics and Reporting の設定タスク フロー

手順

	コマンドまたはアクション	目的
ステップ 1	<p>コール診断の設定 (369 ページ)</p>	<p>このタスクを実行すると、CMR を生成するように Cisco Unified Communications Manager を設定できます。CMR レコードには、コールの音声ストリームの品質に関する情報が格納されます。CDR へのアクセスの詳細については、『<i>Cisco Unified Communications Manager Call Detail Records</i> アドミニストレーションガイド』を参照してください。</p> <p>音声品質メトリックは、Cisco IP Phone で自動的に有効になります。音声品質メトリックへのアクセス方法の詳細については、ご使用の電話機モデルの『<i>Cisco Unified IP Phone</i> アドミニストレーションガイド』を参照してください。</p>
ステップ 2	<p>品質レポート ツールの設定 (369 ページ) を行うには、次のサブタスクを実行します。</p> <ul style="list-style-type: none"> • QRT ソフトキーを含むソフトキーテンプレートの設定 (370 ページ) • 共通デバイス設定と QRT ソフトキーテンプレートの関連付け (372 ページ) • 電話機への QRT ソフトキーテンプレートの追加 (373 ページ) • Cisco Unified Serviceability での QRT の設定 (374 ページ) • 品質レポートツールのサービスパラメータの設定 (377 ページ) 	<p>品質レポートツール(QRT)を設定して、IP phone で問題が発生したユーザが、QRT ソフトキーを押すことによって、問題のタイプやその他の関連統計情報をレポートできるようにします。</p>

コール診断の設定

手順

- ステップ 1** Cisco Unified CM Administration から、[システム (System)] > [サービスパラメータ (Service Parameters)] の順に選択します。
- ステップ 2** [サーバ (Server)] ドロップダウン リストから、Cisco CallManager サービスを実行しているサーバを選択します。
- ステップ 3** [サービス (Service)] ドロップダウン リストから、[Cisco CallManager] を選択します。[サービスパラメータ設定 (Service Parameter Configuration)] ウィンドウが表示されます。
- ステップ 4** [クラスタ全体のパラメータ (デバイス - 全般) (Clusterwide Parameters (Device - General))] エリアで、[コール診断有効 (Call Diagnostics Enabled)] サービスパラメータを設定します。次のオプションを使用できます。

- [無効 (Disabled)] : CMR は生成されません。
- [CDR有効フラグが True の場合のみ有効化 (Enabled Only When CDR Enabled Flag is True)] : [呼詳細レコード (CDR) 有効化フラグ (Call Detail Records (CDR) Enabled Flag)] サービスパラメータが True に設定されている場合のみ、CMR が生成されます。
- [CDR 有効化フラグに関係なく有効化 (Enabled Regardless of CDR Enabled Flag)] : [CDR 有効化フラグ (CDR Enabled Flag)] サービスパラメータの値に関係なく、CMR が生成されます。

(注) [CDR有効化フラグ (CDR Enabled Flag)] サービスパラメータを有効にせずに CMR を生成すると、制御されずにディスク容量が消費される場合があります。CMR を有効にする場合は、CDR を有効にすることをお勧めします。

- ステップ 5** [保存 (Save)] をクリックします。

品質レポート ツールの設定

品質レポートツール(QRT)を設定して、IP phone で問題が発生したユーザが、QRT ソフトキーを押すことによって、問題のタイプやその他の関連統計情報をレポートできるようにします。

手順

	コマンドまたはアクション	目的
ステップ 1	QRT ソフトキーを含むソフトキーテンプレートの設定 (370 ページ)	QRT ソフトキーのオンフック状態と接続済みコール状態を設定する必要があります。次のコール状態も利用できます。 <ul style="list-style-type: none"> • 接続された会議

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> • 接続転送
ステップ 2	<p>(任意) 共通デバイス設定と QRT ソフトキー テンプレートの関連付け (372 ページ) を行うには、次のサブタスクを実行します。</p> <ul style="list-style-type: none"> • 共通デバイス設定への QRT ソフトキーテンプレートの追加 (372 ページ) • 電話機と共通デバイス設定の関連付け (373 ページ) 	<p>ソフトキー テンプレートを電話で使用できるようにするには、この手順か次の手順のいずれかを実行する必要があります。システムが [共通デバイス設定 (Common Device Configuration)] を使用して設定オプションを電話機に適用する場合は、この手順に従います。これは、電話機でソフトキー テンプレートを使用できるようにする際に、最も一般的に使用されている方法です。</p>
ステップ 3	<p>(任意) 電話機への QRT ソフトキー テンプレートの追加 (373 ページ)</p>	<p>次の手順は、ソフトキー テンプレートと共通デバイス設定を関連付けるための代替手段として、または共通デバイス設定と共に使用します。ソフトキー テンプレートを適用して、共通デバイス設定での割り当てや、他のデフォルトのソフトキーの割り当てを上書きする必要がある場合は、次の手順を共通デバイス設定と共に使用します。</p>
ステップ 4	<p>Cisco Unified Serviceability での QRT の設定 (374 ページ) を行うには、次のサブタスクを実行します。</p> <ul style="list-style-type: none"> • Cisco Extended Functions サービスの有効化 (375 ページ) • アラームの設定 (375 ページ) • トレースの設定 (376 ページ) 	
ステップ 5	<p>(任意) 品質レポートツールのサービスパラメータの設定 (377 ページ)</p>	

QRT ソフトキーを含むソフトキー テンプレートの設定

QRT ソフトキーのオンフック状態と接続済みコール状態を設定する必要があります。次のコール状態も利用できます。

- 接続された会議
- 接続転送

手順

-
- ステップ 1** [Cisco Unified CM 管理 (Cisco Unified CM Administration)] から、以下を選択します。[デバイス (Device)] > [デバイスの設定 (Device Settings)] > [ソフトキーテンプレート (Softkey Template)] を選択します。
- ステップ 2** 新しいソフトキーテンプレートを作成するには、この手順を実行します。それ以外の場合は、次のステップに進みます。
- [新規追加 (Add New)] をクリックします。
 - デフォルトのテンプレートを選択して、[コピー (Copy)] をクリックします。
 - [ソフトキーテンプレート名 (Softkey Template Name)] フィールドに、テンプレートの新しい名前を入力します。
 - [保存 (Save)] をクリックします。
- ステップ 3** 既存のテンプレートにソフトキーを追加するには、次の手順を実行します。
- [検索 (Find)] をクリックして、検索条件を入力します。
 - 必要な既存のテンプレートを選択します。
- ステップ 4** [デフォルト ソフトキー テンプレート (Default Softkey Template)] チェックボックスをオンにし、このソフトキーテンプレートをデフォルトのソフトキーテンプレートとして指定します。
- (注) あるソフトキーテンプレートをデフォルトのソフトキーテンプレートとして指定した場合、先にデフォルトの指定を解除してからでないと、そのテンプレートは削除することができません。
- ステップ 5** 右上隅にある [関連リンク (Related Links)] ドロップダウン リストから [ソフトキー レイアウトの設定 (Configure Softkey Layout)] を選択し、[移動 (Go)] をクリックします。
- ステップ 6** [設定するコール状態の選択 (Select a Call State to Configure)] ドロップダウン リストから、ソフトキーに表示するコール状態を選択します。
- ステップ 7** [選択されていないソフトキー (Unselected Softkeys)] リストから追加するソフトキーを選択し、右矢印をクリックして [選択されたソフトキー (Selected Softkeys)] リストにそのソフトキーを移動します。新しいソフトキーの位置を変更するには、上矢印と下矢印を使用します。
- ステップ 8** 追加のコール状態でのソフトキーを表示するには、前述のステップを繰り返します。
- ステップ 9** [保存 (Save)] をクリックします。
- ステップ 10** 次のいずれかの操作を実行します。
- すでにデバイスに関連付けられているテンプレートを変更した場合は、[設定の適用 (Apply Config)] をクリックしてデバイスを再起動します。
 - 新しいソフトキーテンプレートを作成した場合は、そのテンプレートをデバイスに関連付けた後にデバイスを再起動します。詳細については、「共通デバイス設定へのソフトキーテンプレートの追加」と「電話機のセクションとソフトキーテンプレートの関連付け」を参照してください。
-

次のタスク

次のいずれかの手順を実行します。

- [共通デバイス設定への QRT ソフトキー テンプレートの追加 \(372 ページ\)](#)
- [電話機への QRT ソフトキー テンプレートの追加 \(373 ページ\)](#)

共通デバイス設定と QRT ソフトキー テンプレートの関連付け

(オプション) ソフトキー テンプレートを電話機に関連付ける方法は2つあります。

- ソフトキー テンプレートを電話機設定に追加する。
- ソフトキー テンプレートを共通デバイス設定に追加する。

ここに示す手順では、ソフトキーテンプレートを共通デバイス設定に関連付ける方法について説明します。システムが共通デバイス設定を使用して設定オプションを電話機に適用する場合は、この手順に従ってください。これは、電話機でソフトキーテンプレートを使用できるようにする際に、最も一般的に使用されている方法です。

別の方法を使用するには、「[電話機への QRT ソフトキーテンプレートの追加 \(373 ページ\)](#)」を参照してください。

手順

	コマンドまたはアクション	目的
ステップ 1	共通デバイス設定への QRT ソフトキー テンプレートの追加 (372 ページ)	
ステップ 2	電話機と共通デバイス設定の関連付け (373 ページ)	

共通デバイス設定への QRT ソフトキー テンプレートの追加

始める前に

[QRT ソフトキーを含むソフトキーテンプレートの設定 \(370 ページ\)](#)

手順

- ステップ 1 [Cisco Unified CM 管理 (Cisco Unified CM Administration)] から、以下を選択します。[デバイス (Device)] > [デバイスの設定 (Device Settings)] > [共通デバイス設定 (Common Device Configuration)] を選択します。
- ステップ 2 新しい共通デバイス設定を作成し、それにソフトキーテンプレートを関連付けるには、この手順を実行します。それ以外の場合は、次のステップに進みます。
 - a) [新規追加 (Add New)] をクリックします。
 - b) [名前 (Name)] フィールドに、共通デバイス設定の名前を入力します。

c) [保存 (Save)] をクリックします。

ステップ 3 既存の共通デバイス設定にソフトキーテンプレートを追加するには、次の手順を実行します。

- a) [検索 (Find)] をクリックして、検索条件を入力します。
- b) 既存の共通デバイス設定をクリックします。

ステップ 4 [ソフトキーテンプレート (Softkey Template)] ドロップダウンリストで、使用可能にするソフトキーが含まれているソフトキーテンプレートを選択します。

ステップ 5 [保存 (Save)] をクリックします。

ステップ 6 次のいずれかの操作を実行します。

- すでにデバイスに関連付けられている共通デバイス設定を変更した場合は、[設定の適用 (Apply Config)] をクリックしてデバイスを再起動します。
- 新しい共通デバイス設定を作成してその設定をデバイスに関連付けた後に、デバイスを再起動します。

次のタスク

[電話機と共通デバイス設定の関連付け \(373 ページ\)](#)

電話機と共通デバイス設定の関連付け

始める前に

[共通デバイス設定への QRT ソフトキーテンプレートの追加 \(372 ページ\)](#)

手順

ステップ 1 [Cisco Unified CM 管理 (Cisco Unified CM Administration)] から、以下を選択します。[デバイス (Device)] > [電話 (Phone)]。

ステップ 2 [検索 (Find)] をクリックし、ソフトキーテンプレートを追加する電話デバイスを選択します。

ステップ 3 [共通デバイス設定 (Common Device Configuration)] ドロップダウンリストから、新しいソフトキーテンプレートが含まれている共通デバイス設定を選択します。

ステップ 4 [保存 (Save)] をクリックします。

ステップ 5 [リセット (Reset)] をクリックして、電話機の設定を更新します。

電話機への QRT ソフトキーテンプレートの追加

始める前に

[QRT ソフトキーを含むソフトキーテンプレートの設定 \(370 ページ\)](#)

手順

- ステップ 1 [Cisco Unified CM 管理 (Cisco Unified CM Administration)] から、以下を選択します。[デバイス (Device)] > [電話 (Phone)]。
- ステップ 2 [検索 (Find)] をクリックして、設定済みの電話のリストを表示します。
- ステップ 3 電話ボタンテンプレートを追加する電話を選択します。
- ステップ 4 [電話ボタンテンプレート (Phone Button Template)] ドロップダウンリストで、新しい機能ボタンが含まれる電話ボタンテンプレートを選択します。
- ステップ 5 [保存 (Save)] をクリックします。
電話の設定を更新するには [リセット (Reset)] を押すというメッセージ付きのダイアログボックスが表示されます。

Cisco Unified Serviceability での QRT の設定

手順

	コマンドまたはアクション	目的
ステップ 1	Cisco Extended Functions サービスの有効化 (375 ページ)	Cisco 拡張ファンクションサービスをアクティブにすると、品質レポートツールなどの音声品質機能がサポートされます。
ステップ 2	アラームの設定 (375 ページ)	QRT のアラームを設定して、SysLog ビューア内のアプリケーションログのエラーをログに記録します。この機能は、アラームをログに記録し、アラームの説明と推奨される操作を提供します。Syslog ビューアには Cisco Unified Real-Time Monitoring Tool からアクセスできます。
ステップ 3	トレースの設定 (376 ページ)	音声アプリケーションのトレース情報をログに記録するように、QRT のトレースを設定します。QRT のトレースファイルに含める情報を構成したら、Cisco Unified Real-Time 監視ツールのトレースとログセンターオプションを使用して、トレースファイルを収集して表示できます。

Cisco Extended Functions サービスの有効化

Cisco 拡張ファンクションサービスをアクティブにすると、品質レポートツールなどの音声品質機能がサポートされます。

手順

- ステップ 1** Cisco Unified Serviceability から、[ツール (Tools)] > [サービスの有効化 (Service Activation)] 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、Cisco Extended Functionsサービスを有効にするノードを選択します。
- ステップ 3** **Cisco Extended Functions** チェックボックスをオンにします。
- ステップ 4** [保存 (Save)] をクリックします。

次のタスク

[アラームの設定 \(375 ページ\)](#)

アラームの設定

QRT のアラームを設定して、SysLog ビュアー内のアプリケーションログのエラーをログに記録します。この機能は、アラームをログに記録し、アラームの説明と推奨される操作を提供します。Syslog ビュアーにはCisco Unified Real-Time Monitoring Toolからアクセスできます。

始める前に

[Cisco Extended Functions サービスの有効化 \(375 ページ\)](#)

手順

- ステップ 1** Cisco Unified Serviceability で、**アラーム > 設定** 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、ノードを設定するサーバを選択します。
- ステップ 3** サービスグループドロップダウンリストから、**CMサービス**を選択します。
- ステップ 4** [サービス (Service)] ドロップダウンリストから、[Cisco Extended Functions] を選択します。
- ステップ 5** ローカルSyslogsとSDIトレースの両方について**アラームの有効化**チェックボックスをオンにします。
- ステップ 6** このドロップダウンリストから、次のいずれかのオプションを選択し、ローカルSyslogsとSDIトレースの両方にアラームイベントレベルを設定します。
 - **緊急**：このレベルは、システムが使用不可であることを示します。
 - **アラート**：このレベルは、ただちに処置が必要であることを示します。
 - **重要**：システムが重要な状態を検出したことを示します。
 - **エラー**：エラー条件が検出されたことを示します。

- **警告**：このレベルは、警告状態が検出されたことを示します。
- **注意**：通常の重要な条件が検出されていることを示します。
- **情報**：情報メッセージのみを示す。
- **デバッグ**：Cisco技術サポートセンター(TAC)エンジニアにデバッグ用の詳細なイベント情報を指示します。

デフォルト値は **Error** です。

ステップ7 [保存 (Save)] をクリックします。

次のタスク

[トレースの設定 \(376 ページ\)](#)

トレースの設定

音声アプリケーションのトレース情報をログに記録するように、QRT のトレースを設定します。QRTのトレースファイルに含める情報を構成したら、Cisco Unifire Rreal-Time監視ツールのトレースとログセンターオプションを使用して、トレースファイルを収集して表示できます。

始める前に

[アラームの設定 \(375 ページ\)](#)

手順

- ステップ1** Cisco Unified Serviceability から **トレース > 設定** 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、トレースを構成するノードを選択します。
- ステップ3** サービスグループドロップダウンリストから、**CMサービス** を選択します。
- ステップ4** [サービス (Service)] ドロップダウンリストから、[Cisco Extended Functions] を選択します。
- ステップ5** トレースオンチェックボックスをオンにします。
- ステップ6** このドロップダウンリストから、次のいずれかのオプションを選択し、**デバッグトレースレベル**を設定します。
 - **エラー**：すべてのエラー状態、およびプロセスとデバイス初期化メッセージを追跡します。
 - **特殊**：通常運転中に発生したすべての特殊な条件とサブシステムの状態遷移を追跡します。コール処理イベントをトレースします。
 - **状態遷移**：通常の操作中に発生したすべての状態遷移条件とメディア層イベントを追跡します。
 - **重要**：すべての重要条件とルーチンの入り口と出口を追跡します。すべてのサービスがこの追跡レベルを使用するわけではありません。
 - **Entry_exit**：すべての入力条件と終了条件、および基礎となるデバッグ情報を追跡します。
 - **任意**：すべての条件と詳細なデバッグ情報を追跡します。

- **詳細** : アラート状態とイベントを追跡します。異常なパスで生成されたすべてのトレースに使用します。最小の CPU サイクル数を使用します。

デフォルト値は **Error** です。

ヒント トラブルシューティングのためには、このセクションにあるすべてのチェックボックスをオンにするようにしてください。

ステップ 7 [保存 (Save)] をクリックします。

次のタスク

(省略可) [品質レポートツールのサービスパラメータの設定 \(377 ページ\)](#)

品質レポートツールのサービスパラメータの設定



注意 Cisco Technical Assistance Center (TAC) の指示があった場合を除き、デフォルトのサービスパラメータ設定の使用をお勧めします。

手順

-
- ステップ 1** Cisco Unified Communications Manager の管理ページで、**システム > サービスパラメータ** を選択します。
 - ステップ 2** QRT アプリケーションが存在するサーバを選択します。
 - ステップ 3** **Cisco Extended Functions** サービスを選択します。
 - ステップ 4** サービスパラメータを設定します。サービスパラメータとその設定オプションの詳細については、「**関連項目**」セクション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。

関連トピック

[品質レポート ツールのサービス パラメータ \(378 ページ\)](#)

品質レポート ツールのサービス パラメータ

表 78: 品質レポート ツールのサービス パラメータ

パラメータ	説明
拡張 QRT メニューの選択肢を表示する (Display Extended QRT Menu Choices)	<p>拡張メニュー選択項目をユーザに表示するかどうかを決定します。次のいずれかの設定オプションを選択できます。</p> <ul style="list-style-type: none"> このフィールドを [True] に設定すると、拡張メニュー選択項目が表示されます (対話モード)。 このフィールドを [False] に設定すると、拡張メニュー選択項目が表示されません (サイレントモード)。 推奨するデフォルト値として False (サイレントモード) が設定されています。
ストリーミング統計のポーリング期間 (Streaming Statistics Polling Duration)	<p>ストリーミング統計情報のポーリングに使用する間隔を決定します。次のいずれかの設定オプションを選択できます。</p> <ul style="list-style-type: none"> このフィールドを [-1] に設定すると、コールが終了するまでポーリングが行われます。 このフィールドを [0] に設定すると、ポーリングはまったく行われません。 このフィールドを任意の正の値に設定すると、その秒数の間、ポーリングが行われます。コールが終了すると、ポーリングは停止します。 推奨するデフォルトの値として、-1 (コールが終了するまでポーリングを行う) が設定されています。
ストリーミング統計のポーリング頻度 (秒) (Streaming Statistics Polling Frequency (seconds))	<p>ポーリング間に待機する秒数を入力します。</p> <p>値の範囲は、30～3600 です。推奨するデフォルトの値として30が設定されています。</p>

パラメータ	説明
最大ファイル数 (Maximum No. of Files)	<p>ファイルカウントを再起動し、古いファイルを上書きする前に、最大ファイル数を入力します。</p> <p>有効な値は1~1万です。推奨するデフォルトの値は250です。</p>
1 ファイルあたりの最大回線数 (Maximum No. of Lines per File)	<p>各ファイルでの行の最大数を入力します。この数を超えると、次のファイルが始まります。</p> <ul style="list-style-type: none"> • 値の範囲は、100 ~ 2000 です。 • 推奨するデフォルトの値として2000が設定されています。
CTI Managerに安全に接続するためのCAPFプロファイルインスタンスID (CAPF Profile Instance Id for Secure Connection to CTI Manager)	<p>CTI マネージャへのセキュアな接続を開くために Cisco Extended Function サービスが使用する、アプリケーションユーザ CCMQRTSysUser の CAPF アプリケーションプロファイルのインスタンス ID を入力します。CTI Manager Connection Security Flag パラメータが有効な場合、このパラメータを設定する必要があります。</p> <p>(注) CTI Manager Connection Security Flag サービスパラメータを有効にすることで、セキュリティをオンにします。変更を有効にするためには、Cisco Extended Functions サービスを再起動する必要があります。</p>
CTI Manager接続セキュリティフラグ (CTI Manager Connection Security Flag)	<p>Cisco Extended Functions サービスの CTI Manager 接続のセキュリティを有効にするか、または無効にするかを選択します。有効にすると、Cisco Extended Functions はアプリケーションユーザ CCMQRTSysUser のインスタンス ID に設定された CAPF アプリケーションプロファイルを使用して、CTI マネージャへのセキュアな接続を開きます。</p> <p>値は True または False を選択します。CTI へのセキュアな接続を有効にするには、True を選択する必要があります。</p>



第 VI 部

セキュリティの管理

- [SAML シングルサインオンの管理 \(383 ページ\)](#)
- [証明書の管理 \(393 ページ\)](#)
- [一括証明書の管理 \(413 ページ\)](#)
- [IPSec ポリシーの管理 \(417 ページ\)](#)
- [クレデンシャル ポリシーの管理 \(421 ページ\)](#)



第 24 章

SAML シングル サインオンの管理

- [SAML シングル サインオンの概要 \(383 ページ\)](#)
- [iOS 上での Cisco Jabber の証明書ベースの SSO 認証のオプトイン制御 \(383 ページ\)](#)
- [SAML シングル サインオンの前提条件 \(384 ページ\)](#)
- [SAML シングル サインオンの管理 \(385 ページ\)](#)

SAML シングル サインオンの概要

定義された一連の Cisco アプリケーションのうちの 1 つにサインインした後は、SAML シングルサインオン (SSO) を使用して、それらすべてのアプリケーションにアクセスできます。SAML では、信頼できるビジネス パートナー間で、セキュリティに関連した情報交換を記述します。これは、ユーザを認証するために、サービス プロバイダー (Cisco Unified Communications Manager など) が使用する認証プロトコルです。SAML では、ID プロバイダー (IdP) とサービス プロバイダーとの間でセキュリティ認証情報が交換されます。この機能は、さまざまなアプリケーションにわたり、共通の資格情報と関連情報を使用するための安全な機構を提供します。

SAML SSO は、IdP とサービス プロバイダーの間でのプロビジョニング プロセスの一部として、メタデータと証明書を交換することで、信頼の輪 (CoT) を確立します。サービス プロバイダーは IdP のユーザ情報を信頼して、さまざまなサービスやアプリケーションへのアクセスを許可します。

クライアントは IdP に対する認証を行い、IdP はクライアントにアサーションを与えます。クライアントはサービス プロバイダーにアサーションを提示します。CoT が確立されているため、サービス プロバイダーはアサーションを信頼し、クライアントにアクセス権を与えます。

iOS 上での Cisco Jabber の証明書ベースの SSO 認証のオプトイン制御

このリリースの Cisco Unified Communications Manager には、iOS での Cisco Jabber の SSO ログイン動作を ID プロバイダー (IdP) によって制御するためのオプトイン設定オプションが導入

されています。このオプションを使用すると、制御されたモバイル デバイス管理 (MDM) 環境内で、Cisco Jabber が IdP による証明書ベースの認証を実行できるようになります。

オプトイン制御を設定するには、Cisco Unified Communications Manager で [iOS の SSO ログイン動作 (SSO Login Behavior for iOS)] エンタープライズ パラメータを使用します。



- (注) このパラメータのデフォルト値を変更する前に、<http://www.cisco.com/c/en/us/support/unified-communications/jabber-windows/tsd-products-support-series-home.html> で Cisco Jabber 機能のサポートおよびドキュメントを参照して、SSO ログイン動作と証明書ベースの認証に対する iOS 上での Cisco Jabber のサポートを確認してください。

この機能を有効にするには、[iOS Cisco Jabber の SSO ログインの動作設定 \(386 ページ\)](#) の手順を参照してください。

SAML シングル サインオンの前提条件

- Cisco Unified Communications Manager クラスタに DNS が設定されていること
- ID プロバイダー (IdP) サーバ
- IdP サーバによって信頼され、システムでサポートされる LDAP サーバ

SAML SSO 機能のテストは、SAML 2.0 を使用した以下の IdP で行われています。

- OpenAM 10.0.1
- Microsoft[®] Active Directory[®] Federation Services 2.0 (AD FS 2.0)
- PingFederate[®] 6.10.0.4
- F5 BIP-IP 11.6.0

サードパーティ アプリケーションは、次の設定要件を満たす必要があります。

- 必須属性の「uid」が IdP で設定されていること。この属性は、Cisco Unified Communications Manager の LDAP と同期されたユーザ ID に使用されている属性と一致している必要があります。
- SAML SSO に参加するすべてのエンティティのクロックを同期させる必要があります。クロックの同期の詳細については、『*System Configuration Guide for Cisco Unified Communications Manager*』 (<http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html>) の「[NTP Settings]」を参照してください。

SAML シングル サインオンの管理

SAML シングル サインオンの有効化



(注) 同期エージェントの確認テストに合格するまで、SAML SSOを有効にすることができません。

始める前に

- ユーザデータが Unified Communications Manager データベースに同期されていることを確認します。詳細については、<http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html> で、『*System Configuration Guide for Cisco Unified Communications Manager*』を参照してください。
- Cisco Unified CM IM and Presence サービスと Cisco Sync Agent サービスのデータ同期が完了していることを確認します。このテストのステータスをチェックするには、**[Cisco Unified CM IM and Presence Administration]** > **[診断 (Diagnostics)]** > **[システム トラブルシューター (System Troubleshooter)]** を選択します。[Sync Agent が関連データ (デバイス、ユーザ、ライセンス情報など) を使用して同期したことを確認する (Verify Sync Agent has sync'ed over relevant data (e.g. devices, users, licensing information))] 「」 テストは、データ同期が正常に完了した場合にテスト合格の結果が示されています。
- Cisco Unified CM の管理へのアクセスを有効にするには、少なくとも 1 人の LDAP 同期ユーザが Standard CCM Super Users グループに追加されていることを確認します。詳細については、<http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html> で、『*System Configuration Guide for Cisco Unified Communications Manager*』を参照してください。
- IdP とサーバ間の信頼関係を設定するには、IdP から信頼メタデータ ファイルを取得し、それをすべてのサーバにインポートする必要があります。

手順

- ステップ 1 Cisco Unified CM の管理で、**[システム (System)]** > **[SAML シングルサインオン (SAML Single Sign-On)]** を選択します。
- ステップ 2 **[SAML SSO の有効化 (Enable SAML SSO)]** をクリックします。
- ステップ 3 すべてのサーバ接続が再起動されることを通知する警告メッセージが表示されたら、**[続行 (Continue)]** をクリックします。
- ステップ 4 **[参照 (Browse)]** をクリックし、IdP メタデータ ファイルを探してアップロードします。

- ステップ 5 [IdP メタデータのインポート (Import IdP Metadata)] をクリックします。
- ステップ 6 [次へ (Next)] をクリックします。
- ステップ 7 [信頼メタデータ ファイルセットのダウンロード (Download Trust Metadata Fileset)] をクリックして、サーバメタデータをシステムにダウンロードします。
- ステップ 8 IdP サーバ上にサーバメタデータをアップロードします。
- ステップ 9 [次へ (Next)] をクリックして続行します。
- ステップ 10 有効な管理者 ID のリストから、管理者権限を持つ LDAP 同期ユーザを選択します。
- ステップ 11 [テストを実行 (Run Test)] をクリックします。
- ステップ 12 有効なユーザ名およびパスワードを入力します。
- ステップ 13 成功メッセージが表示されたら、ブラウザ ウィンドウを閉じます。
- ステップ 14 [完了 (Finish)] をクリックし、Web アプリケーションが再起動するまで 1~2 分待ちます。

iOS Cisco Jabber の SSO ログインの動作設定

手順

- ステップ 1 Cisco Unified CM Administration から、[システム (System)] > [エンタープライズパラメータ (Enterprise Parameters)] を選択します。
- ステップ 2 オプトイン制御を設定するには、[SSOの設定 (SSO Configuration)] セクションで、[iOS向け SSOログイン動作 (SSO Login Behavior for iOS)] パラメータで、[ネイティブブラウザの使用 (Use Native Browser)] オプションを選択します。
- (注) [iOS向け SSOログイン動作 (SSO Login Behavior for iOS)] パラメータには次のオプションが含まれます。
- [組み込みブラウザの使用 (Use Embedded Browser)] : このオプションを有効にすると、Cisco Jabber は SSO の認証に、組み込みブラウザを使用します。このオプションにより、バージョン 9 より前の iOS デバイスのネイティブ Apple Safari ブラウザで、クロス起動なしの SSO を使用できるようになります。このオプションは、デフォルトで有効です。
 - [ネイティブブラウザの使用 (Use Native Browser)] : このオプションを有効にすると、Cisco Jabber は、iOS デバイスで Apple Safari フレームワークを使用し、MDM の導入で、ID プロバイダー (IdP) を利用する証明書ベースの認証を実行します。
- (注) ネイティブブラウザの使用は組み込みブラウザの使用ほど安全ではないため、制御された MDM の導入での利用を除いては、このオプションの設定を推奨しません。

ステップ 3 [保存 (Save)] をクリックします。

アップグレード後の WebDialer 上での SAML シングル サインオンの有効化

次のタスクに従って、アップグレード後に Cisco WebDialer 上で SAML シングル サインオンを再度アクティブ化します。SAML シングル サインオンを有効化する前に Cisco WebDialer をアクティブ化すると、デフォルトで、Cisco WebDialer 上で SAML シングル サインオンが有効になりません。

手順

	コマンドまたはアクション	目的
ステップ 1	Cisco WebDialer サービスの非アクティブ化 (387 ページ)	Cisco WebDialer Web サービスがすでにアクティブになっている場合は、それを非アクティブにします。
ステップ 2	SAML シングル サインオンの無効化 (388 ページ)	SAML シングル サインオンがすでに有効になっている場合は、それを無効にします。
ステップ 3	Cisco WebDialer サービスのアクティブ化 (388 ページ)	
ステップ 4	SAML シングル サインオンの有効化 (385 ページ)	

Cisco WebDialer サービスの非アクティブ化

Cisco WebDialer Web サービスがすでにアクティブになっている場合は、それを非アクティブにします。

手順

- ステップ 1 Cisco Unified Serviceability から、[ツール (Tools)] > [サービスの有効化 (Service Activation)] を選択します。
- ステップ 2 [サーバ (Servers)] ドロップダウンリストから、リストされている Cisco Unified Communications Manager サーバを選択します。
- ステップ 3 [CTI サービス (CTI Services)] で、[Cisco WebDialer Web サービス (Cisco WebDialer Web Service)] チェック ボックスをオフにします。
- ステップ 4 [保存 (Save)] をクリックします。

次のタスク

[SAML シングル サインオンの無効化 \(388 ページ\)](#)

SAML シングル サインオンの無効化

SAML シングル サインオンがすでに有効になっている場合は、それを無効にします。

始める前に

[Cisco WebDialer サービスの非アクティブ化 \(387 ページ\)](#)

手順

CLI から、**utils sso disable** コマンドを実行します。

次のタスク

[Cisco WebDialer サービスのアクティブ化 \(388 ページ\)](#)

Cisco WebDialer サービスのアクティブ化

始める前に

[SAML シングル サインオンの無効化 \(388 ページ\)](#)

手順

-
- ステップ 1 [Cisco Unified Serviceability] から選択します。[ツール (Tools)] > [サービス アクティベーション (Service Activation)] を選択します。
 - ステップ 2 [サーバ (Server)] ドロップダウン リストから、リストされている Unified Communications Manager サーバを選択します。
 - ステップ 3 [CTI サービス (CTI Services)] から、[Cisco WebDialer Web サービス (Cisco WebDialer Web Service)] チェック ボックスをオンにします。
 - ステップ 4 [保存 (Save)] をクリックします。
 - ステップ 5 [Cisco Unified Serviceability] から選択します。[ツール (Tools)] > [コントロール センター - 機能サービス (Control Center - Feature Services)] を選択して、CTI Manager サービスがアクティブでスタート モードになっていることを確認します。

WebDialer を正しく機能させるには、CTI Manager サービスをアクティブにして、スタート モードにする必要があります。

次のタスク

[SAML シングル サインオンの有効化 \(385 ページ\)](#)

リカバリ URL へのアクセス

トラブルシューティングのために、SAML シングル サインオンをバイパスして、Cisco Unified Communications Manager Administration インターフェイスと Cisco Unified CM IM and Presence サービス インターフェイスにログインする場合に、リカバリ URL を使用します。たとえば、サーバのドメインまたはホスト名を変更する前に、リカバリ URL を有効にします。リカバリ URL にログインすると、サーバメタデータの更新が容易になります。

始める前に

- 管理権限を持っているアプリケーションユーザのみがリカバリ URL にアクセスできます。
- SAML SSO が有効になっている場合は、リカバリ URL がデフォルトで有効になります。CLI からリカバリ URL を有効/無効にすることができます。リカバリ URL を有効または無効にする CLI コマンドの詳細については、『*Command Line Interface Guide for Cisco Unified Communications Solutions*』を参照してください。

手順

ブラウザで、「`https://hostname:8443/ssosp/local/login`」と入力します。

ドメインまたはホスト名変更後のサーバメタデータの更新

ドメインまたはホスト名の変更後は、この手順を実行するまで、SAML シングル サインオンが機能しません。



-
- (注) この手順を実行しても [SAML シングル サインオン (SAML Single Sign-On)] ウィンドウにログインできない場合は、ブラウザのキャッシュをクリアしてもう一度ログインしてみてください。
-

始める前に

リカバリ URL が無効になっている場合、シングルサインオンリンクをバイパスするようには表示されません。リカバリ URL を有効にするには、CLI にログインして次のコマンドを実行します：**`utils sso recovery-url enable`**。

手順

-
- ステップ 1** Web ブラウザのアドレス バーに次の URL を入力します。
- ```
https://<Unified CM-server-name>
```
- <Unified CM-server-name> はホスト名またはサーバの IP アドレスです。
- ステップ 2** [シングルサインオンをバイパスするリカバリ URL (Recovery URL to bypass Single Sign-On (SSO)) ] をクリックします。
- ステップ 3** 管理者ロールを持つアプリケーションユーザのクレデンシャルを入力し、[ログイン (Login) ] をクリックします。
- ステップ 4** Cisco Unified CM の管理で、[システム (System) ]>[SAML シングルサインオン (SAML Single Sign-On) ] を選択します。
- ステップ 5** [メタデータのエクスポート (Export Metadata) ] をクリックしてサーバメタデータをダウンロードします。
- ステップ 6** サーバメタデータ ファイルを IdP にアップロードします。
- ステップ 7** [テストを実行 (Run Test) ] をクリックします。
- ステップ 8** 有効なユーザ ID とパスワードを入力します。
- ステップ 9** 成功のメッセージが表示されたら、ブラウザウィンドウを閉じます。
- 

## サーバー削除後にサーバーのメタデータを更新する

クラスタ全体の SSO 統合でサーバーがクラスタから削除された後、IdP とのインデックスの不一致を避けるためにメタデータの再インポートが必須です。

### Before you begin



**Note** リカバリ URL が無効になっている場合、シングルサインオンリンクをバイパスするようには表示されません。リカバリ URL を有効にするには、CLI にログインして次のコマンドを実行します：**utils sso recovery-url enable**。

---

### Procedure

- 
- ステップ 1** Web ブラウザのアドレス バーに次の URL を入力します。
- ```
https://<Unified CM-server-name>
```
- <Unified CM-server-name> はホスト名またはサーバの IP アドレスです。
- ステップ 2** [シングルサインオンをバイパスするリカバリ URL (Recovery URL to bypass Single Sign-On (SSO))] をクリックします。

- ステップ3 管理者ロールを持つアプリケーションユーザのクレデンシャルを入力し、[ログイン (Login)] をクリックします。
- ステップ4 Cisco Unified CM Administration で、[システム (System)] > [SAML シングルサインオン (SAML Single Sign-On)] を選択します。
- ステップ5 [メタデータのエクスポート (Export Metadata)] をクリックしてサーバメタデータをダウンロードします。
- ステップ6 サーバメタデータ ファイルを IdP にアップロードします。
- ステップ7 [テストを実行 (Run Test)] をクリックします。
- ステップ8 有効なユーザ ID とパスワードを入力します。
- ステップ9 成功のメッセージが表示されたら、ブラウザウィンドウを閉じます。

サーバメタデータの手動プロビジョニング

ID プロバイダーで複数の UC アプリケーション用の単一接続をプロビジョニングするには、ID プロバイダーとサービス プロバイダー間の信頼の輪を設定しながら、サーバメタデータを手動でプロビジョニングする必要があります。信頼の輪の設定方法については、IdP 製品のマニュアルを参照してください。

一般的な URL 構文は次のとおりです。

```
https://<SP FQDN>:8443/ssosp/saml/SSO/alias/<SP FQDN>
```

手順

サーバメタデータを手動でプロビジョニングするには、Assertion Customer Service (ACS) URL を使用します。

例：

```
サンプル ACS URL : <md:AssertionConsumerService  
Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"  
Location="https://cucm.ucsso.cisco.com:8443/ssosp/saml/SSO/alias/cucm.ucsso.cisco.com"  
index="0"/>
```




第 25 章

証明書管理

- [証明書の概要 \(393 ページ\)](#)
- [証明書の表示 \(397 ページ\)](#)
- [証明書のダウンロード \(398 ページ\)](#)
- [中間証明書のインストール \(398 ページ\)](#)
- [信頼証明書の削除 \(399 ページ\)](#)
- [証明書の再作成 \(400 ページ\)](#)
- [証明書または証明書チェーンのアップロード \(403 ページ\)](#)
- [サードパーティ証明書の認証局の管理 \(404 ページ\)](#)
- [オンライン証明書ステータスプロトコル \(OCSP\) による証明書失効 \(CRL\) \(407 ページ\)](#)
- [証明書モニタリングタスクフロー \(409 ページ\)](#)
- [証明書エラーのトラブルシューティング \(411 ページ\)](#)

証明書の概要

システムでは、自己署名証明書とサードパーティの署名付き証明書が使用されます。送信元から宛先までのデータ整合性を確保するために、デバイスのセキュア認証、データの暗号化、データのハッシュを行う際に、システム内のデバイス間で証明書を使用します。証明書を使用することにより、帯域幅、通信、操作のセキュアな転送が可能になります。

証明書を使用する際、意図した Web サイト、電話、FTP サーバなどのエンティティとの間でデータがどのように暗号化され共有されているかを理解し、それを定義することが最も重要な部分です。

システムが証明書を信頼するということは、システムにプレインストールされている証明書によって、適切な接続先と情報を共有していることが完全に確信されているということです。そうでない場合、システムはこれらのポイント間の通信を終了します。

証明書を信頼するには、サードパーティ認証局 (CA) によって信頼がすでに確立されている必要があります。

まずデバイスが CA 証明書と中間証明書の両方を信頼できると認識していることが必要であり、そうであるならデバイスは Secure Socket Layer (SSL) ハンドシェイクというメッセージの交換によって提供されるサーバ証明書を信頼することができます。



- (注) Tomcat 用の EC ベースの証明書がサポートされています。この新しい証明書を tomcat-ECDSA といいます。詳細については、『*Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager*』の「Enhanced TLS Encryption on IM and Presence Service」の章を参照してください。

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。

EC ベースの証明書の詳細については、Cisco Unified Communications Manager and IM and Presence Service 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。

サードパーティの署名付き証明書または証明書チェーン

アプリケーション証明書に署名した認証局の認証局ルート証明書をアップロードします。下位認証局がアプリケーション証明書に署名した場合は、下位認証局の認証局ルート証明書をアップロードする必要があります。すべての認証局証明書の PKCS#7 形式の証明書チェーンもアップロードできます。

認証局ルート証明書およびアプリケーション証明書は、同じ [証明書のアップロード (Upload Certificate)] ダイアログボックスを使用してアップロードできます。認証局ルート証明書または認証局証明書だけが含まれる証明書チェーンをアップロードする場合は、certificate type-trust 形式の証明書名を選択します。アプリケーション証明書またはアプリケーション証明書と認証局証明書が含まれる証明書チェーンをアップロードする場合は、証明書タイプだけが含まれている証明書名を選択します。

たとえば、Tomcat 認証局証明書または認証局証明書チェーンをアップロードする場合は [tomcat-trust] を選択します。Tomcat アプリケーション証明書またはアプリケーション証明書と認証局証明書が含まれる証明書チェーンをアップロードする場合は、[tomcat] または [tomcat-ECDSA] を選択します。

CAPF 認証局ルート証明書をアップロードすると、CallManager の信頼ストアにコピーされるため、認証局ルート証明書を個別に CallManager にアップロードする必要はありません。



- (注) サードパーティの認証局署名付き証明書が正常にアップロードされると、署名付き証明書を取得するために使用された、最近生成した CSR が削除され、サードパーティの署名付き証明書 (アップロードされている場合) を含む既存の証明書が上書きされます。



(注) tomcat-trust、CallManager-trust、および Phone-SAST-trust 証明書がクラスタの各ノードに自動的にレプリケートされます。



(注) DirSync サービスをセキュア モードで実行する場合に必要なディレクトリの信頼証明書は、tomcat-trust にアップロードすることができます。

サードパーティ認証局証明書

サードパーティ認証局が発行するアプリケーション証明書を使用するには、署名付きのアプリケーション証明書と認証局ルート証明書の両方を認証局から取得するか、アプリケーション証明書と認証局証明書の両方が含まれている PKCS#7 証明書チェーン (Distinguished Encoding Rules [DER]) から取得する必要があります。これらの証明書の取得に関する情報は、認証局から入手してください。証明書を取得するプロセスは、認証局によって異なります。署名アルゴリズムでは RSA 暗号化が使用されている必要があります。

Cisco Unified Communications オペレーティングシステムでは、プライバシー強化メール (PEM) エンコード形式で CSR が作成されます。システムは、DER および PEM エンコード形式の証明書と、PEM 形式の PKCS#7 証明書チェーンを受け入れます。認証局プロキシ機能 (CAPF) 以外のすべての証明書タイプの場合、それぞれのノードについて認証局ルート証明書およびアプリケーション証明書を取得してアップロードする必要があります。

CAPF の場合、最初のノードについてのみ認証局ルート証明書およびアプリケーション証明書を取得してアップロードします。CAPF および Unified Communications Manager の CSR には、認証局へのアプリケーション証明書要求に含める必要のある拡張情報が含まれています。認証局が拡張要求メカニズムをサポートしていない場合は、次の手順に従って X.509 拡張を有効にする必要があります。

- CAPF CSR では、次の拡張情報が使用されます。

X509v3 拡張キーの使用： TLS Web サーバ認証、X509v3 キーの使用： デジタル署名、証明書署名

- Tomcat および Tomcat-ECDSA の CSR では、次の拡張情報が使用されます。



(注) Tomcat または Tomcat-ECDSA は、キー アグリーメントや IPsec エンドシステム キーを使用する必要はありません。

X509v3 拡張キー使用： TLS Web サーバ認証、TLS Web クライアント認証、IPsec エンドシステム X509v3 キー使用： デジタル署名、キー暗号化、データ暗号化、キー同意

- IPsec の CSR では、次の拡張情報が使用されます。

X509v3 拡張キー使用： TLS Web サーバ認証、TLS Web クライアント認証、IPSec エンドシステム X509v3 キー使用： デジタル署名、キー暗号化、データ暗号化、キー同意

- Unified Communications Manager の CSR では、次の拡張情報が使用されます。

X509v3 拡張キー使用： TLS Web サーバ認証、TLS Web クライアント認証 X509v3 キー使用： デジタル署名、キー暗号化、データ暗号化、キー同意

- IM and Presence Service cup および cup-xmpp 証明書の CSR は、次の拡張機能を使用します。

X509v3 拡張キー使用： TLS Web サーバ認証、TLS Web クライアント認証、IPSec エンドシステム X509v3 キー使用： デジタル署名、キー暗号化、データ暗号化、キー アグリーメント



(注) 使用する証明書に対して CSR を生成し、SHA256 署名を使用してサードパーティ認証局に署名させることもできます。この署名付き証明書を Unified Communications Manager に再度アップロードすることで、Tomcat および他の証明書が SHA256 をサポートできるようになります。

証明書署名要求のキー用途拡張

次の表には、Unified Communications Manager と IM and Presence Service の CA 証明書の証明書署名要求 (CSR) のキーの用途拡張が表示されています。

表 79: Cisco Unified Communications Manager CSR キーの用途拡張

	マルチサーバ	キーの拡張用途			キーの用途				
		サーバ認証 (1.3.6.1.5.5.7.3.1)	クライアント 認証 (1.3.6.1.5.5.7.3.2)	IP セキュリ ティ 末端シス テム (1.3.6.1.5.5.7.3.5)	デジタル署名	鍵の暗号化	データの暗号 化	キー証明書署 名	鍵共有
CallManager CallManager-ECDSA	Y	Y	Y		Y	N	Y		
CAPF (パブリッシャ のみ)	N	Y	N		Y	N		Y	
ipsec	N	Y	Y	Y	Y	Y	Y		
tomcat tomcat-ECDSA	Y	Y	Y		Y	N	Y		
信頼検証サービス (TVS)	N	Y	Y		Y	Y	Y		

表 80 : IM and Presence Service CSR キーの用途拡張

	マルチサーバ	キーの拡張用途			キーの用途				
		サーバ認証 (1.3.6.1.5.5.7.3.1)	クライアント 認証 (1.3.6.1.5.5.7.3.2)	IP セキュリ ティ 末端シス テム (1.3.6.1.5.5.7.3.5)	デジタル署名	鍵の暗号化	データの暗号 化	キー証明書署 名	鍵共有
cup cup-ECDSA	N	Y	Y	Y	Y	Y	Y		
cup-xmpp cup-xmpp-ECDSA	Y	Y	Y	Y	Y	Y	Y		
cup-xmpp-s2s cup-xmpp-s2s-ECDSA	Y	Y	Y	Y	Y	Y	Y		
ipsec	N	Y	Y	Y	Y	Y	Y		
tomcat tomcat-ECDSA	Y	Y	Y		Y	Y	Y		



(注) CA 署名証明書のプロセスの一部として、「データ暗号化」ビットが変更または削除されていないことを確認します。

証明書の表示

証明書の一覧を共通名、有効期限、キータイプ、使用法に基づいて並べ替えて表示するには、[証明書の一覧 (Certificate List)] ページでフィルタオプションを使用します。フィルタオプションにより、データの並べ替え、表示、管理を効率的に行うことができます。

Unified Communications Manager リリース 14 以降では、アイデンティティ証明書または信頼証明書の一覧を並べ替えて表示するときの基準として、使用法オプションを選択できます。

手順

- ステップ 1** Cisco Unified OS の管理から、[セキュリティ (Security)] > [証明書の管理 (Certificate Management)] を選択します。
[Certificate List] ページが表示されます。
- ステップ 2** [証明書の一覧の検索条件 (Find Certificate List where)] ドロップダウンリストから目的のフィルタオプションを選択し、[検索 (Find)] フィールドに検索項目を入力して、[検索 (Find)] ボタンをクリックします。

たとえば、アイデンティティ証明書だけを表示するには、[証明書の一覧の検索条件 (Find Certificate List where)] ドロップダウンリストから [使用法 (Usage)] を選択し、[検索 (Find)] フィールドにアイデンティティを入力して、[検索 (Find)] ボタンをクリックします。

BCFIPS プロバイダーの証明書表示データは、リリース 14SU2 以降で変更されました。

14SU1 までのタグ名	14SU2 からのタグ名
発行者名	発行者 DN
有効期限	開始日
送信先	最終日
サブジェクト名	サブジェクト DN
キー	公開キー (3Public Key)
キー値	モジュラス

(注) x509 拡張機能は、実際のキー使用法名ではなく OID 名で表示されます。

証明書のダウンロード

CSR 要求を送信する場合は、ダウンロード証明書タスクを使用して証明書のコピーを作成するか、証明書をアップロードします。

手順

- ステップ 1 [Cisco Unified OS Administration] から [セキュリティ (Security)] > [証明書の管理 (Certificate Management)] を選択します。
- ステップ 2 検索情報を指定し、[検索 (Find)] をクリックします。
- ステップ 3 必要なファイル名を選択し、[ダウンロード (Download)] をクリックします。

中間証明書のインストール

中間証明書をインストールするには、まずルート証明書をインストールしてから、署名付き証明書をアップロードする必要があります。この手順は、認証局から 1 つの署名付き証明書と複数の証明書が証明書チェーンで提供している場合にのみ必要です。

手順

-
- ステップ 1** [Cisco Unified OS の管理 (Cisco Unified OS Administration)] から、[セキュリティ (Security)] > [証明書の管理 (Certificate Management)] をクリックします。
- 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** ルート証明書をインストールするには、[証明書の目的 (Certificate Purpose)] ドロップダウンリストから適切な信頼ストアを選択します。
- ステップ 4** 選択した証明書の目的の説明を入力します。
- ステップ 5** 次のいずれかの手順を実行して、アップロードするファイルを選択します。
- [ファイルのアップロード (Upload File)] テキストボックスに、ファイルへのパスを入力します。
 - [参照 (Browse)] をクリックしてファイルに移動し、[開く (Open)] をクリックします。
- ステップ 6** [アップロード (Upload)] をクリックします。
- ステップ 7** 顧客証明書をインストールしたら、FQDN を使用して Cisco Unified Intelligence Center の URL にアクセスします。IP アドレスを使用して Cisco Unified Intelligence Center にアクセスすると、カスタム証明書を正常にインストールした後でも「ここをクリックしてログインを続けます (Click here to continue)」のメッセージが表示されます。「」
- (注)
 - Tomcat 証明書をアップロードするときは、TFTP サービスを再起動します。それ以外の場合は、TFTP は古いキャッシュの自己署名された tomcat 証明書を提供し続けます。
-

信頼証明書の削除

削除できる証明書は、信頼できる証明書だけです。システムで生成される自己署名証明書は削除できません。



-
- 注意** 証明書を削除すると、システムの動作に影響する場合があります。また、証明書が既存のチェーンの一部である場合、証明書チェーンが壊れることがあります。この関係は、[証明書の一覧 (Certificate List)] ウィンドウ内の関連する証明書のユーザ名とサブジェクト名から確認します。この操作は取り消すことができません。
-

手順

-
- ステップ 1** [Cisco Unified OS の管理 (Cisco Unified OS Administration)] から [セキュリティ (Security)] > [証明書の管理 (Certificate Management)] を選択します。
- ステップ 2** 証明書の一覧をフィルタするには、[検索 (Find)] コントロールを使用します。
- ステップ 3** 証明書のファイル名を選択します。
- ステップ 4** [削除 (Delete)] をクリックします。
- ステップ 5** [OK] をクリックします。

- (注)
- 削除する証明書が「CAPF-trust」、「tomcat-trust」、「CallManager-trust」、または「Phone-SAST-trust」証明書タイプの場合、証明書はクラスタ内のすべてのサーバで削除されます。
 - 証明書を CAPF-trust にインポートする場合、それはその特定のノードでのみ有効になり、クラスタ全体で複製されることはありません。
-

証明書の再作成

証明書が期限切れになる前に、証明書を再生成することを推奨します。RTMT (Syslog Viewer) で警告が発行され、証明書の期限が近くなると電子メールで通知が送信されます。

ただし、期限切れの証明書を再生成することもできます。電話機を再起動してサービスを再起動する必要があるため、営業時間後にこのタスクを実行します。Cisco Unified OS の管理に「cert」タイプとしてリストされている証明書のみ再作成できます。



注意 証明書を再作成すると、システムの動作に影響する場合があります。証明書を再作成すると、サードパーティの署名付き証明書 (アップロードされている場合) を含む既存の証明書が上書きされます。

手順

-
- ステップ 1** [Cisco Unified OS の管理 (Cisco Unified OS Administration)] から [セキュリティ (Security)] > [証明書の管理 (Certificate Management)] を選択します。
- 検索パラメータを入力して、証明書を検索して設定の詳細を表示します。すべての条件に一致したレコードが [Certificate List] ウィンドウに表示されます。
- 証明書の詳細ページで [再生成 (Regenerate)] ボタンをクリックすると、同じキー長を持つ自己署名証明書が再生成されます。

(注) 証明書を再生成する場合、[再生成 (Regeneration)] ウィンドウを閉じて、新しく生成された証明書を開くまで、[証明書の説明 (Certificate Description)] フィールドは更新されません。

3072 または 4096 の新しいキー長の自己署名証明書を再生成するには、[自己署名証明書の生成 (Generate Self-Signed Certificate)] をクリックします。

ステップ 2 [自己署名証明書の新規作成 (Generate New Self-Signed Certificate)] ウィンドウのフィールドを設定します。フィールドとその設定オプションの詳細については、オンラインヘルプを参照してください。

ステップ 3 [生成 (Generate)] をクリックします。

ステップ 4 再作成された証明書の影響を受けるサービスをすべて再起動します。詳細については、[証明書の名前と説明 \(401 ページ\)](#) を参照してください。

ステップ 5 CAPF 証明書、ITLRecovery 証明書、または CallManager 証明書の再生成後に CTL ファイルを更新します (設定している場合)。

(注) 証明書を再作成したら、システムのバックアップを実行して、最新のバックアップに再作成した証明書が含まれるようにします。バックアップに再作成した証明書が含まれていない状態でシステムの復元タスクを実行する場合は、システム内の各電話機のロックを手動で解除して、電話機を登録できるようにする必要があります。

証明書の名前と説明

次の表に、再作成可能なシステムのセキュリティ証明書と、再起動する必要がある関連サービスを示します。TFTP 証明書の再作成の詳細については、<http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html> の『Cisco Unified Communications Manager Security Guide』を参照してください。

表 81: 証明書の名前と説明

名前	説明	再起動サービス
tomcat tomcat-ECDSA	この証明書は、SIP Oauth モードが有効な場合に Web サービス、Cisco DRF サービス、および Cisco CallManager サービスで使用されます。	tomcat - Cisco Cisco Disaster (DRS) ロー サービス。 tomcat-ECDSA サービス。
ipsec	この自己署名ルート証明書は、Unified Communications Manager、MGCP、H.323、および IM and Presence サービスとの IPsec 接続のインストール中に生成されます。	IPsec サービス

名前	説明	再起動サービス
CallManager CallManager-ECDSA	SIP、SIP トランク、SCCP、TFTP などに使用されます。	CallManager - 該 CallManager-EC CallManager サー サービス、TFTP
CAPF	Unified Communications Manager パブリッシャで実行されている CAPF サービスで使用されます。この証明書は、エンドポイントに LSC を発行するために使用されます（オンラインおよびオフライン CAPF モードを除く）。	該当なし
信頼検証サービス (TVS)	これは信頼検証サービスで使用され、サーバ証明書が変更された場合に、電話機のセカンダリ信頼検証メカニズムとして機能します。	該当なし



- (注)
- [セキュリティパラメータ (Security Parameter)] セクションには、新しいエンタープライズパラメータとして [証明書更新時の電話機の動作 (Phone Interaction on Certificate Update)] が導入され、TVS、CAPF、TFTP のいずれかの証明書が更新されたときに、電話機のリセットを手動で行うか自動で行うかを設定できます。デフォルトでは、このパラメータは電話機を自動的にリセットするように設定されています。
 - 証明書の再生成、削除、および更新後、「再起動サービス」の列に記載されている適切なサービスを再起動してください。



重要 この注記は、リリース 14SU2 にのみ適用されます。

リリース 14SU2 の場合、Cisco DRF サービスは、Tomcat-ECDSA 証明書の再生成またはアップロード後に再起動する必要があります。Tomcat RSA 証明書操作後に再起動する必要はありません。

OAuth 更新ログイン用のキーの再生成

コマンドラインインターフェイスを使用して暗号キーと署名キーの両方を再生成するには、この手順を使用します。Cisco Jabber が Unified Communications Manager との OAuth 認証に使用する暗号キーまたは署名キーが侵害された場合にのみ、この作業を実行します。署名キーは非対称で RSA ベースであるのに対し、暗号キーは対称キーです。

このタスクを完了すると、これらのキーを使用する現在のアクセストークンと更新トークンは無効になります。

エンドユーザへの影響を最小限に抑えるために、このタスクは営業時間外に完了することを推奨します。

暗号キーは、以下の CLI を使用してのみ再生成できますが、パブリッシャノードの Cisco Unified OS の管理 GUI を使用して署名キーを再生成することもできます。[**セキュリティ (Security)**] > [**証明書の管理 (Certificate Management)**] を選択し、**AUTHZ** 証明書を選択して、[**再作成 (Regenerate)**] をクリックします。

手順

ステップ 1 Unified Communications Manager パブリッシャノードで、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 暗号キーを再生成するには、次の手順を実行します。

- a) `set key regen authz encryption` コマンドを実行します。
- b) 「yes」と入力します。

ステップ 3 署名キーを再生成するには、次の手順を実行します。

- a) `set key regen authz signing` コマンドを実行します。
- b) 「yes」と入力します。

Unified Communications Manager パブリッシャ ノードがキーを再生成し、IM and Presence サービスのローカルノードを含めたすべての Unified Communications Manager クラスタ ノードに新しいキーを複製します。

すべての UC クラスタで新しいキーを再生成して同期する必要があります。

- **IM and Presence 中央クラスタ** : IM and Presence 集中型展開の場合、IM and Presence ノードはテレフォニーとは別のクラスタ上で実行されています。この場合、IM and Presence Service の中央クラスタの Unified Communications Manager パブリッシャ ノードで、この手順を繰り返します。
- **Cisco Expressway または Cisco Unity Connection** : これらのクラスタ上でもキーを再生成します。詳細については、Cisco Expressway および Cisco Unity Connection のマニュアルを参照してください。

(注) 次のシナリオでは、Cisco XCP 認証サービスを再起動する必要があります。

- Authz 証明書を再生成する場合
- IM and Presence 管理コンソールで集中型展開に新しいエントリを作成する場合

証明書または証明書チェーンのアップロード

システムで信頼する新しい証明書または証明書チェーンをアップロードします。

手順

- ステップ1 Cisco Unified OS の管理から、[セキュリティ (Security)] > [証明書の管理 (Certificate Management)] を選択します。
- ステップ2 [証明書/証明書チェーンのアップロード (Upload Certificate/Certificate chain)] をクリックします。
- ステップ3 [証明書の用途 (Certificate Purpose)] ドロップダウンリストで、証明書名を選択します。
- ステップ4 次のいずれかの手順を実行して、アップロードするファイルを選択します。
- [ファイルのアップロード (Upload File)] テキストボックスに、ファイルへのパスを入力します。
 - [参照 (Browse)] をクリックしてファイルに移動してから、[開く (Open)] をクリックします。
- ステップ5 ファイルをサーバにアップロードするには、[ファイルのアップロード (Upload File)] をクリックします。
- (注) 証明書をアップロードしたら、影響を受けるサービスを再起動します。サーバが再起動したら、CCMAdmin または CCMUser GUI にアクセスして、新しく追加した証明書が使用されていることを確認できます。

サードパーティ証明書の認証局の管理

このタスクフローでは、サードパーティ証明書プロセスの概要を、各ステップへの参照とともに順番に説明します。お使いのシステムは、サードパーティ認証局が PKCS # 10 証明書署名要求 (CSR) を使用して発行する証明書をサポートしています。

手順

	コマンドまたはアクション	目的
ステップ1	証明書署名要求の生成 (405 ページ)	証明書署名要求 (CSR) を生成します。これは、公開キー、組織名、共通名、地域、および国などの証明書申請情報を含む暗号化されたテキストのブロックです。認証局はこの CSR を使用して、ご使用のシステムの信頼できる証明書を生成します。
ステップ2	証明書署名要求のダウンロード (406 ページ)	CSR を生成した後にダウンロードし、認証局に提出する準備をします。

	コマンドまたはアクション	目的
ステップ 3	認証局のドキュメントを参照してください。	認証局からアプリケーション証明書を取得します。
ステップ 4	認証局のドキュメントを参照してください。	認証局からルート証明書を取得します。
ステップ 5	信頼ストアへの認証局署名済み CAPF ルート証明書の追加 (406 ページ)	ルート証明書を信頼ストアに追加します。認証局の署名付き CAPF 証明書を使用している場合は、この手順を実行します。
ステップ 6	証明書または証明書チェーンのアップロード (403 ページ)	認証局ルート証明書をノードにアップロードします。
ステップ 7	CAPF または Cisco Unified Communications Manager の証明書を更新した場合は、新しい CTL ファイルを生成します。	『Cisco Unified Communications Manager Security Guide』 (http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html) を参照してください。 サードパーティの署名付き CAPF または CallManager 証明書をアップロードしたら、CTL クライアント (設定している場合) を再実行します。
ステップ 8	サービスの再起動 (407 ページ)	新しい証明書の影響を受けるサービスを再起動します。すべての証明書タイプで、対応するサービスを再起動します (たとえば、Tomcat または Tomcat-ECDSA の証明書を更新した場合は Cisco Tomcat サービスを再起動します)。

証明書署名要求の生成

証明書署名要求 (CSR) を生成します。これは、公開キー、組織名、共通名、地域、および国などの証明書申請情報を含む暗号化されたテキストのブロックです。認証局はこの CSR を使用して、ご使用のシステムの信頼できる証明書を生成します。



(注) 新しい CSR を生成すると、既存の CSR は上書きされます。

手順

-
- ステップ1 Cisco Unified OS の管理から、[セキュリティ (Security)] > [証明書の管理 (Certificate Management)] を選択します。
 - ステップ2 [CSR の作成 (Generate CSR)] をクリックします。
 - ステップ3 [証明書署名要求の作成 (Generate Certificate Signing Request)] ウィンドウのフィールドを設定します。フィールドとその設定オプションの詳細については、オンラインヘルプを参照してください。
 - ステップ4 [生成 (Generate)] をクリックします。
-

証明書署名要求のダウンロード

CSR を生成した後にダウンロードし、認証局に提出する準備をします。

手順

-
- ステップ1 [Cisco Unified OS Administration] から [セキュリティ (Security)] > [証明書の管理 (Certificate Management)] を選択します。
 - ステップ2 [CSR のダウンロード (Download CSR)] をクリックします。
 - ステップ3 [証明書の用途 (Certificate Purpose)] ドロップダウンリストで、証明書名を選択します。
 - ステップ4 [CSR のダウンロード (Download CSR)] をクリックします。
 - ステップ5 (任意) プロンプトが表示されたら、[保存 (Save)] をクリックします。
-

信頼ストアへの認証局署名済み CAPF ルート証明書の追加

認証局署名済み CAPF ルート証明書を使用する場合は、ルート証明書を Unified Communications Manager 信頼ストアに追加します。

手順

-
- ステップ1 Cisco Unified OS の管理から、[セキュリティ (Security)] > [証明書の管理 (Certificate Management)] を選択します。
 - ステップ2 [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/証明書チェーンのアップロード (Upload Certificate/Certificate chain)] ポップアップウィンドウで、[証明書の目的 (Certificate Purpose)] ドロップダウンリストから [CallManager-trust] を選択し、認証局署名済み CAPF ルート証明書を参照します。

ステップ 4 [ファイルのアップロード (UploadFile)]フィールドに証明書が表示されたら、[アップロード (Upload)]をクリックします。

サービスの再起動

クラスタ内の特定のノードで機能またはネットワーク サービスを再起動する必要がある場合は、次の手順に従います。

手順

ステップ 1 再起動するサービスのタイプに応じて、次のいずれかのタスクを実行します。

- [ツール (Tools)] > [コントロール センター - 機能サービス (Control Center - Feature Services)] の順に選択します。
- [ツール (Tools)] > [コントロール センター - ネットワーク サービス (Control Center - Network Services)] を選択します。

ステップ 2 [サーバ (Server)] ドロップダウンリストからシステム ノードを選択し、[移動 (Go)] をクリックします。

ステップ 3 再起動するサービスの横にあるオプションボタンをクリックし、[再起動 (Restart)] をクリックします。

ステップ 4 再起動にはしばらく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。

オンライン証明書ステータス プロトコル (OCSP) による 証明書失効 (CRL)

Unified Communications Manager は、証明書失効を監視するための OCSP をプロビジョニングします。システムは証明書のステータスをチェックして、スケジュールされた間隔での有効性を確認します。また、証明書がアップロードされるたびに確認します。

Online Certificate Status Protocol (OCSP) は、管理者がシステムの証明書要件を管理するのに役に立ちます。OCSP が設定されている場合、証明書の有効性をチェックし、期限切れの証明書をリアルタイムで失効させるためのシンプルでセキュアな自動化された方法を提供します。

共通基準モードが有効になっている FIPS 展開では、OCSP によって、システムが一般的な基準要件に準拠することもできます。

有効性検査

Unified Communications Manager は、証明書のステータスを確認し、有効性を確認します。

証明書は次のように検証されます。

- Unified Communications Manager は代理信頼モデル (DTM) を使用し、OCSP 署名属性のルート CA または中間 CA をチェックします。ルート CA または中間 CA は、OCSP 証明書に署名してステータスを確認する必要があります。委任された信頼モデルに障害が発生した場合、Unified Communications Manager は信頼応答側モデル (TRP) にフォールバックし、OCSP サーバからの指定された OCSP 応答署名証明書を使用して証明書を検証します。



(注) 証明書の失効ステータスを確認するには、OCSP 応答側が実行されている必要があります。

- [証明書失効 (Certificate 失効)] ウィンドウの OCSP オプションを有効にして、証明書失効をリアルタイムで確認する最も安全な方法を提供します。証明書または設定された OCSP URI から OCSP URI を使用する場合は、[from options] を選択します。OCSP の手動設定の詳細については、「OCSP を使用した [OCSP による証明書失効の設定](#)」を参照してください。



(注) リーフ証明書の場合、syslog、FileBeat、SIP、ILS、LBM などの TLS クライアントは ocsd 要求を ocsd 応答側に送信し、ocsd 応答側からリアルタイムで証明書失効応答を受信します。

検証が実行され、共通基準モードがオンになると、次のいずれかのステータスが証明書に返されます。

- **良好 (Good)** : 良好な状態とは、ステータスの問い合わせへの肯定的な応答を示します。少なくとも、この正の応答は、証明書が失効していないことを示しますが、必ずしも証明書が発行されたか、または応答が生成された時刻が証明書の有効期間内であることを意味するわけではありません。応答拡張機能は、発行、有効性などの陽性ステートメントなど、応答側によって発行されたアサーションに関する追加情報を、証明書のステータスについて伝えるために使用される場合があります。
- **失効 (Revoked)** : 失効状態は、証明書が失効していることを示します (permanently または一時的に保留中のいずれか)。
- **不明 (Unknown)** : 不明状態は、OCSP 応答側が要求されている証明書について認識していないことを示します。



- (注) 一般的な基準モードでは、接続は失効した場合と不明な場合の両方で失敗しますが、一般的な基準が有効になっていない場合、接続は不明な応答ケースで成功します。

証明書モニタリング タスク フロー

次のタスクを行い、証明書ステータスと有効期限を自動的にモニタするようシステムを設定します。

- 証明書の有効期限が近づいているときは、電子メールで通知する。
- 有効期限が切れた証明書を失効させる。

手順

	コマンドまたはアクション	目的
ステップ 1	証明書モニタ通知の設定 (409 ページ)	証明書の自動モニタリングを構成します。システムは定期的に証明書ステータスをチェックし、証明書の有効期限が近づいていると電子メールで通知します。
ステップ 2	OCSP による証明書失効の設定 (410 ページ)	期限切れの証明書が自動的に失効するように OCSP を設定します。

証明書モニタ通知の設定

Unified Communications Manager または IM and Presence サービスの自動証明書モニタリングを設定します。システムは定期的に証明書のステータスをチェックし、証明書の有効期限が近づいていると電子メールで通知します。



- (注) [Cisco Certificate Expiry Monitor] ネットワーク サービスを実行している必要があります。デフォルトでこのサービスは有効化されていますが、[ツール (Tools)] > [コントロール センター - ネットワーク サービス (Control Center - Network Services)] を選択し、[Cisco Certificate Expiry Monitor サービス (Cisco Certificate Expiry Monitor Service)] の状態が [実行中 (Running)] であることを検証して Cisco Unified Serviceability でサービスが実行中であることを確認できます。

手順

- ステップ 1 (Unified Communications Manager の証明書モニタリングのために) Cisco Unified OS の管理にログインするか、(IM and Presence サービスの証明書モニタリングのために) Cisco Unified IM and Presence の管理にログインします。
- ステップ 2 [セキュリティ (Security)] > [証明書モニタ (Certificate Management)] を選択します。
- ステップ 3 [通知開始時期 (Notification Start Time)] フィールドに、数値を入力します。この値は、近づきつつある有効期限の通知を、有効期限の何日前にシステムが開始するかを表します。
- ステップ 4 [通知頻度 (Notification Frequency)] フィールドには、通知を行う頻度を入力します。
- ステップ 5 これはオプションです。[電子メール通知を有効にする (Enable E-mail notification)] チェックボックスをオンにして、近づきつつある証明書有効期限に関する電子メールアラートをシステムに送信させます。
- ステップ 6 [LSC モニタリングを有効にする (Enable LSC Monitoring)] チェックボックスをオンにして、LSC 証明書を証明書ステータスチェックに含めます。
- ステップ 7 [電子メール ID (E-mail IDs)] フィールドに、システムが通知を送信する電子メールアドレスを入力します。複数の電子メールアドレスは、セミコロンで区切って入力できます。
- ステップ 8 [保存 (Save)] をクリックします。

(注) 証明書モニタ サービスは、デフォルトで 24 時間ごとに 1 回だけ実行します。証明書モニタ サービスを再起動すると、サービスが開始され、24 時間後に実行する次のスケジュールが計算されます。証明書の有効期限が 7 日以内に近づいても、この周期は変化しません。このサービスは、証明書の有効期限が切れる 1 日前から、有効期限が切れた後も 1 時間おきに実行します。

次のタスク

Online Certificate Status Protocol (OCSP) を設定し、期限切れの証明書をシステムが自動的に失効させるようにします。詳細については、次を参照してください。[OCSP による証明書失効の設定 \(410 ページ\)](#)

OCSP による証明書失効の設定

オンライン証明書ステータスプロトコル (OCSP) を有効にして、証明書の状態を定期的にチェックし、期限切れの証明書を自動的に失効させます。

始める前に

システムに OCSP チェックに必要な証明書があることを確認します。OCSP 応答属性を設定されているルート CA 証明書または中間 CA 証明書を使用することができます。または、tomcat-trust へアップロードされている指定された OCSP 署名証明書を使用することができます。

手順

- ステップ 1** (Unified Communications Manager の証明書失効のために) Cisco Unified OS の管理にログインするか、(IM and Presence サービスの証明書失効のために) Cisco Unified IM and Presence の管理にログインします。
- ステップ 2** [セキュリティ (Security)] > [証明書失効 (Certificate Revocation)] を選択します。
- ステップ 3** [OCSP の有効化 (Enable OCSP)] チェック ボックスをオンにして、次のタスクのいずれかを実行します。
- OCSP チェックの OCSP レスポンダを指定する場合は、[設定済み OCSP URI を使用する (Use configured OCSP URI)] ボタンを選択し、[OCSP 設定済み URI (OCSP Configured URI)] フィールドにレスポンスの URI を入力します。
 - OCSP レスポンダ URI で証明書を設定する場合、[証明書からの OCSP URI を使用する (Use OCSP URI from Certificate)] ボタンを選択します。
- ステップ 4** [失効チェックを有効にする (Enable Revocation Check)] チェック ボックスをオンにします。
- ステップ 5** [チェック間隔 (Check Every)] フィールドに失効チェックの間隔を入力します。
- ステップ 6** [保存 (Save)] をクリックします。
- ステップ 7** (省略可) CTI、IPsec または LDAP リンクがある場合は、これらの長期性接続の OCSP 失効サポートを有効にするために、上記の手順に加えて次の手順も行う必要があります。
- a) Cisco Unified CM の管理から、[システム (System)] > [エンタープライズ パラメータ (Enterprise Parameters)] を選択します。
 - b) [証明書の失効や有効期限 (Certificate Revocation and Expiry)] で、[証明書有効性チェック (Certificate Validity Check)] パラメーターを [True] に設定します。
 - c) [有効性チェック頻度 (Validity Check Frequency)] パラメーターの値を設定します。
(注) 証明書失効ウィンドウの [失効チェックを有効にする (Enable Revocation Check)] パラメーターの間隔値は、[有効性チェック頻度 (Validity Check Frequency)] エンタープライズ パラメーターの値よりも優先されます。
 - d) [保存 (Save)] をクリックします。

証明書エラーのトラブルシュート

始める前に

IM and Presence サービス ノードから Unified Communications Manager サービスに、または、Unified Communications Manager ノードから IM and Presence サービス機能にアクセスしようとしてエラーが発生した場合は、tomcat-trust 証明書に問題があります。「サーバへの接続を確立できません (リモート ノードに接続できません) (Connection to the Server cannot be established (unable to connect to Remote Node))」というエラー メッセージが、次の [サービスアビリティ (Serviceability)] インターフェイス ウィンドウに表示されます。

- [サービスのアクティブ化 (Service Activation)]
- コントロールセンター - 機能サービス
- コントロールセンター - ネットワーク サービス

この手順を使用して、証明書のエラーを解決します。最初のステップから開始し、必要に応じて進みます。最初のステップだけでエラーが解決される場合もあれば、すべてのステップを実行することが必要になる場合もあります。

手順

-
- ステップ 1** [Cisco Unified OS の管理 (Cisco Unified OS Administration)] の [セキュリティ (Security)] > [証明書の管理 (Certificate Management)] で、必要な tomcat-trust 証明書が存在することを確認します。
- 必要な証明書がない場合は、再度確認するまで 30 分間待ちます。
- ステップ 2** 証明書を選択して情報を表示します。証明書の内容が、リモートノード上の対応する証明書の内容と一致することを確認します。
- ステップ 3** CLI から、**utils service restart Cisco Intercluster Sync Agent** を実行して Cisco Intercluster Sync Agent サービスを再起動します。
- ステップ 4** Cisco Intercluster Sync Agent サービスが再起動したら、**utils service restart Cisco Tomcat** を実行して Cisco Tomcat サービスを再起動します。
- ステップ 5** 30 分間待機します。前の手順で証明書のエラーが対処されず、tomcat-trust 証明書が存在する場合は、証明書を削除します。証明書を削除したら、ノードごとに Tomcat および Tomcat-ECDSA 証明書をダウンロードし、tomcat-trust 証明書としてピアにアップロードすることで、証明書を手動で交換する必要があります。
- ステップ 6** 証明書の交換が完了したら、**utils service restart Cisco Tomcat** を実行して、影響を受ける各サーバで Cisco Tomcat を再起動します。
-



第 26 章

一括証明書の管理

- [一括証明書の管理 \(413 ページ\)](#)

一括証明書の管理

クラスタ間で証明書のセットを共有する場合に、一括証明書管理を使用します。この手順は、Extension Mobility Cross Cluster などのクラスタ間で信頼を確立する必要があるシステム機能に必要です。

手順

	コマンドまたはアクション	目的
ステップ 1	証明書のエクスポート (413 ページ)	この手順では、クラスタ内の全ノードの証明書を含む PKCS12 ファイルを作成します。
ステップ 2	証明書のインポート (414 ページ)	ホーム クラスタとリモート (訪問先) クラスタに証明書をインポートします。

証明書のエクスポート

この手順では、クラスタ内の全ノードの証明書を含む PKCS12 ファイルを作成します。

手順

- ステップ 1** [Cisco Unified OS の管理 (Cisco Unified OS Administration)] から、[セキュリティ (Security)] > [証明書の一括管理 (Bulk Certificate Management)] を選択します。
- ステップ 2** ホーム クラスタとリモート クラスタの両方で到達可能な TFTP サーバを設定します。フィールドとその設定オプションの詳細については、オンライン ヘルプを参照してください。
- ステップ 3** [保存 (Save)] をクリックします。

ステップ4 [エクスポート (Export)]をクリックします。

ステップ5 [証明書の一括エクスポート (Bulk Certificate Export)]ウィンドウの[証明書のタイプ (Certificate Type)]フィールドで、[すべて (All)]を選択します。

ステップ6 [エクスポート (Export)]をクリックします。

ステップ7 [Close] をクリックします。

(注) 一括証明書エクスポートを実行すると、証明書は次のようにリモートクラスタにアップロードされます。

- CAPF 証明書は Callmanager-trust としてアップロードされます。
- Tomcat 証明書は Tomcat-trust としてアップロードされます
- CallManager 証明書は Callmanager-trust としてアップロードされます
- CallManager 証明書は Phone-SAST-trust としてアップロードされます
- ITLRecovery 証明書は、PhoneSast-trust および CallManager-trust としてアップロードされます。

上記の手順は、証明書が自己署名され、別のクラスタに共通の信頼がない場合に実行されます。共通の信頼関係または同じ署名者がいる場合は、すべての証明書のエクスポートは必要ありません。

証明書のインポート

ホームクラスタとリモート（訪問先）クラスタに証明書をインポートします。



(注) 一括証明書管理機能を使用して証明書をインポートすると、電話機がリセットされます。

始める前に

[インポート (Import)] ボタンが表示されるには、次の操作を完了しておく必要があります。

- 2つ以上のクラスタから SFTP サーバに証明書をエクスポートします。
- エクスポートした証明書を統合します。

手順

ステップ1 [Cisco Unified OSの管理 (Cisco Unified OS Administration)]から、以下を選択します。[セキュリティ (Security)]> [証明書の一括管理 (Bulk Certificate Management)]> [インポート (Import)]> [証明書の一括インポート (Bulk Certificate Import)]を選択します。

ステップ2 [証明書タイプ (Certificate Type)] ドロップダウンリストから、[すべて (All)] を選択します。

ステップ3 [Import] を選択します。

(注) 一括証明書インポートを実行すると、証明書は次のようにリモートクラスタにアップロードされます。

- CAPF 証明書は Callmanager-trust としてアップロードされます。
- Tomcat 証明書は Tomcat-trust としてアップロードされます
- CallManager 証明書は Callmanager-trust としてアップロードされます
- CallManager 証明書は Phone-SAST-trust としてアップロードされます
- ITLRecovery 証明書は、PhoneSast-trust および CallManager-trust としてアップロードされます。

(注) 次のタイプの証明書により、再起動する電話が決定されます。

- Callmanager : TFTP サービスが、証明書が属するノード上でアクティブになっている場合にのみ、すべての電話。
 - TV : Callmanager グループ メンバーシップに基づいて、一部の電話。
 - CAPF : CAPF がアクティブになっている場合にのみ、すべての電話。
-



第 27 章

IPSec ポリシーの管理

- [IPsec ポリシーの概要 \(417 ページ\)](#)
- [IPsec ポリシーの設定 \(418 ページ\)](#)
- [IPsec 証明書の確認, on page 419](#)
- [IPSec ポリシーの管理 \(419 ページ\)](#)

IPsec ポリシーの概要

IPsec は、暗号セキュリティサービスを使用した IP ネットワーク経由の非公開でセキュアな通信を保証するフレームワークです。IPsec ポリシーが IPsec セキュリティ サービスの設定に使用されます。このポリシーは、ネットワーク上のほとんどのトラフィックタイプにさまざまなレベルの保護を提供します。コンピュータ、部門 (OU)、ドメイン、サイト、またはグローバル企業のセキュリティ要件を満たすように IPsec ポリシーを設定できます。

IPsec ポリシーの設定



- (注)
- システムアップグレード中に IPsec ポリシーに対して行った変更は無効となるので、アップグレード中は IPsec ポリシー を修正または作成しないでください。
 - IPsec には双方向プロビジョニングが必要です（ホストまたはゲートウェイごとに 1 ピア）。
 - 一方の IPsec ポリシー プロトコルが「ANY」、もう一方の IPsec ポリシー プロトコルが「UDP」または「TCP」に設定されている 2 つの Unified Communications Manager ノードに IPsec ポリシーをプロビジョニングする場合、「ANY」プロトコルを使用するノードでの検証で検出漏れが発生する可能性があります。
 - IPsec はシステムのパフォーマンスに影響します（特に暗号化した場合）。
 - IPsec ポリシーが現在のバージョンまたはアップグレードされたバージョンで構成されていますが、基本バージョンで構成されていない場合は、このバージョンを基本バージョンに切り替えるときに、IPsec ポリシーを削除するか無効にしてください。これは、いずれかのノードのみで IPsec ポリシーが構成され、両方のバージョンをスイッチバックするまで、他ノードには、IPsec ポリシーが構成されないためです。そうしないと、接続の問題が発生します。
 - Unified CM ノードの再起動後、IPsec 接続が起動していない場合は、**utils ipsec restart** コマンドを使用して IPsec サービスを再起動し、IPsec 接続を正常に確立してください。この回避策は、ネットワーク接続が確立される前に IPsec サービスを再起動する際の問題を軽減するために行います。

手順

- ステップ 1 Cisco Unified OS の管理から [セキュリティ (Security)] > [IPsec の設定 (IPSec Configuration)] 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 [IPSEC ポリシーの設定 (IPSEC Policy Configuration)] ウィンドウで各フィールドを設定します。フィールドとその設定オプションの詳細については、オンラインヘルプを参照してください。
- ステップ 4 [保存 (Save)] をクリックします。
- ステップ 5 (任意) IPsec を検証するには、[サービス (Services)] > [Ping] の順に選択し、[IPsec の検証 (Validate IPsec)] チェックボックスをオンにして、[Ping] をクリックします。

IPsec 証明書の確認

次の手順を使用して、IPsec 証明書を確認します。

Procedure

- ステップ 1 [Cisco Unified OS の管理 (Cisco Unified OS Administration)] から [セキュリティ (Security)] > [管理証明書 (Management Certificate)] を選択します。
- ステップ 2 検索情報を指定し、[検索 (Find)] をクリックします。
- ステップ 3 IPsec 証明書を検索します (パブリッシャノードとサブスクライバノードに個別にログインします)。

Note 通常、サブスクライバノードの IPsec 証明書はパブリッシャノードで表示できません。ただし、パブリッシャノードの IPsec 証明書は、IM&P ノードのサブスクライバノードで表示できます。

IPsec 接続を有効にするには、一方のノードからの CA 署名付き IPsec 証明書を、もう一方のノードの **IPsec-Trust** 証明書として使用する必要があります。

新しい証明書を **IPsec-Trust** にアップロードする前に、**IPsec-Trust** で同じ共通名を持つ以前の証明書を削除する必要があります。

IPSec ポリシーの管理

システムのアップグレード中、IPSec ポリシーに何らかの変更を行ってもその変更は無効になります。アップグレード中は IPSec ポリシーを変更または作成しないでください。



注意 ホスト名、ドメイン、または IP アドレスを変更するために既存の IPSec 証明書に変更を加える際、証明書名を変更する場合は、IPSec ポリシーを削除して作り直す必要があります。証明書名を変更しない場合は、リモート ノードの作り直した証明書をインポートした後に、IPSec ポリシーを無効にして有効にする必要があります。

手順

- ステップ 1 Cisco Unified OS の管理から [セキュリティ (Security)] > [IPSec の設定 (IPSec Configuration)] の順に選択します。
- ステップ 2 ポリシーを表示、イネーブル、またはディセーブルにするには、次の手順を実行します。
 - a) ポリシー名をクリックします。

- b) ポリシーを有効または無効にするには、[ポリシーの有効化 (Enable Policy)] チェックボックスをオンまたはオフにします。
- c) [保存 (Save)] をクリックします。
- d) ポリシーを無効にする場合、無効化の変更を有効にするには、**utils ipsec restart** コマンドを実行する必要があります。

ステップ 3 1 つまたは複数のポリシーを削除するには、次の手順を実行します。

- a) 削除するポリシーの横にあるチェックボックスをオンにします。
[すべてを選択 (Select All)] をクリックするとすべてのポリシーを選択でき、[すべてをクリア (Clear All)] を選択するとすべてのチェックボックスをクリアできます。
 - b) [選択項目の削除 (Delete Selected)] をクリックします。
-



第 28 章

クレデンシャルポリシーの管理

- [クレデンシャルポリシーと認証 \(421 ページ\)](#)
- [クレデンシャルポリシーの設定 \(422 ページ\)](#)
- [クレデンシャルポリシー デフォルトの設定 \(423 ページ\)](#)
- [認証アクティビティのモニタ \(423 ページ\)](#)
- [クレデンシャルキャッシングの設定 \(425 ページ\)](#)
- [セッションの終了の管理 \(425 ページ\)](#)

クレデンシャルポリシーと認証

認証機能は、ユーザの認証、クレデンシャル情報の更新、ユーザイベントとエラーのトラッキングとロギング、クレデンシャル変更履歴の記録、データストレージ用のユーザクレデンシャルの暗号化または復号を行います。

システムは常に、アプリケーションユーザパスワードとエンドユーザ PIN を Unified Communications Manager データベースに照合します。エンドユーザパスワードについては、社内ディレクトリまたはデータベースに照合して認証できます。

システムが社内ディレクトリと同期されていれば、Unified Communications Manager または Lightweight Directory Access Protocol (LDAP) のいずれかの認証機能によってパスワードを認証できます。

- LDAP 認証が有効にされている場合、ユーザパスワードおよびクレデンシャルポリシーは適用されません。これらのデフォルトは、ディレクトリ同期 (DirSync サービス) で作成されたユーザに適用されます。
- LDAP 認証を無効にすると、システムはユーザクレデンシャルをデータベースに照合して認証します。このオプションを使用する場合、クレデンシャルポリシーを割り当て、認証イベントおよびパスワードを管理することができます。エンドユーザは、電話機のユーザインターフェイスでパスワードと PIN を変更できます。

クレデンシャルポリシーは、オペレーティングシステムのユーザまたは CLI のユーザには適用されません。オペレーティングシステムの管理者は、オペレーティングシステムでサポートされている標準のパスワード検証手順を使用します。

ユーザがデータベースに設定された後、ユーザが各自のクレデンシャルを変更するよう要求されたときに、以前の情報を入力することを防ぐために、システムはデータベースにユーザクレデンシャルの履歴を保存します。

クレデンシャルポリシーの JTAPI および TAPI のサポート

Cisco Unified Communications Manager Java テレフォニー アプリケーション プログラミング インターフェイス (JTAPI) およびテレフォニー アプリケーション プログラミング インターフェイス (TAPI) は、アプリケーションユーザに割り当てられたクレデンシャルポリシーをサポートするため、開発者はパスワードの有効期限、PIN の有効期限、およびクレデンシャルポリシーの適用のためのロックアウト戻りコードに応答するアプリケーションを作成する必要があります。

アプリケーションは、アプリケーションが使用する認証モデルに関係なく、API を使用してデータベースまたは社内ディレクトリで認証します。

開発者向けの JTAPI および TAPI の詳細については、開発者ガイド (<http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-programming-reference-guides-list.html>) を参照してください。

クレデンシャルポリシーの設定

クレデンシャルポリシーは、アプリケーションユーザとエンドユーザに適用されます。パスワードポリシーをエンドユーザとアプリケーションユーザに割り当て、PIN ポリシーをエンドユーザに割り当てます。[クレデンシャルポリシーのデフォルトの設定 (Credential Policy Default Configuration)] に、これらのグループのポリシー割り当てが一覧表示されます。新しいユーザをデータベースに追加すると、システムがデフォルトポリシーを割り当てます。割り当てられたポリシーを変更したり、ユーザ認証イベントを管理したりできます。



- (注) CTI アプリケーションユーザーに対して、クレデンシャルポリシー設定の下の [許可される非アクティブ日数 (Inactive Days Allowed)] パラメータが 0 (制限なし) に設定されていることを確認します。そうしないと、アプリケーションユーザーが予期せず非アクティブになり、再起動後に CTI アプリケーションが Unified CM に接続できないことがあります。

手順

ステップ 1 Cisco Unified CM Administration から、[ユーザの管理 (User Management)] > [ユーザ設定 (User Settings)] > [クレデンシャルポリシー (Credential Policy)] を選択します。

ステップ 2 次のいずれかの手順を実行します。

- [検索 (Find)] をクリックし、既存のクレデンシャルポリシーを選択します。
- [新規追加 (Add New)] をクリックして、新しいクレデンシャルポリシーを作成します。

- ステップ 3** [クレデンシャルポリシーの設定 (Credential Policy Configuration)] ウィンドウの各フィールドに入力します。フィールドとその設定の詳細については、オンラインヘルプを参照してください。
- ステップ 4** [保存 (Save)] をクリックします。

クレデンシャルポリシー デフォルトの設定

インストール時に、Cisco Unified Communications Manager がスタティック デフォルト クレデンシャル ポリシーをユーザ グループに割り当てます。デフォルト クレデンシャルは提供しません。お使いのシステムが、新しいデフォルト ポリシーを割り当てたり、ユーザの新しいデフォルト クレデンシャルとクレデンシャル要件を設定したりするためのオプションを提供します。

手順

- ステップ 1** Cisco Unified CM Administration で、[ユーザの管理 (User Management)] > [ユーザ設定 (User Settings)] > [クレデンシャルポリシーデフォルト (Credential Policy Default)] を選択します。
- ステップ 2** [クレデンシャルポリシー (Credential Policy)] ドロップダウン リスト ボックスから、このグループのクレデンシャル ポリシーを選択します。
- ステップ 3** [クレデンシャルの変更 (Change Credential)] と [クレデンシャルの確認 (Confirm Credential)] の両方にパスワードを入力します。
- ステップ 4** このクレデンシャルをユーザに変更させない場合は、[ユーザは変更不可 (User Cannot Change)] チェックボックスをオンにします。
- ステップ 5** ユーザが次のログイン時に変更する必要がある、一時的なクレデンシャルを設定する場合は、[次回ログイン時に変更必要 (User Must Change at Next Login)] チェックボックスをオンにします。
- (注) このボックスをオンにすると、ユーザはパーソナル ディレクトリ サービスを使用して PIN を変更できなくなることに注意してください。
- ステップ 6** クレデンシャルの期限を設定しない場合は、[有効期限なし (Does Not Expire)] チェックボックスをオンにします。
- ステップ 7** [保存 (Save)] をクリックします。

認証アクティビティのモニタ

システムは、最後のハッキング試行時刻や失敗したログイン試行のカウントなどの最新の認証結果を表示します。

システムは、次のクレデンシャル ポリシー イベントに関するログ ファイル エントリを生成します。

- 認証成功
- 認証失敗（不正なパスワードまたは不明）
- 次の原因による認証失敗
 - 管理ロック
 - ハッキング ロック（失敗したログオン ロックアウト）
 - 期限切れソフト ロック（期限切れのクレデンシャル）
 - 非アクティブ ロック（一定期間使用されていないクレデンシャル）
 - ユーザによる変更が必要（ユーザが変更するように設定されたクレデンシャル）
 - LDAP 非アクティブ（LDAP 認証へ切り替えたものの LDAP が非アクティブ）
- 成功したユーザ クレデンシャル更新
- 失敗したユーザ クレデンシャル更新



(注) エンド ユーザ パスワードに対して LDAP 認証を使用する場合は、LDAP は認証の成功と失敗だけを追跡します。

すべてのイベント メッセージに、文字列「ims-auth」と認証を試みているユーザ ID が含まれています。

手順

- ステップ 1** [Cisco Unified CM の管理 (Cisco Unified CM Administration)] [ユーザの管理 (User Management)] > [エンド ユーザ (End Users)] を選択します。
- ステップ 2** 検索条件を入力し、[検索 (Find)] をクリックして、表示された一覧からユーザを選択します。
- ステップ 3** [クレデンシャルの編集 (Edit Credential)] をクリックし、ユーザの認証アクティビティを表示します。

次のタスク

Cisco Unified Real-Time Monitoring Tool (Unified RTMT) を使用してログ ファイルを表示できます。また、キャプチャしたイベントをレポートに収集できます。Unified RTMT の詳細な使用手順については、『Cisco Unified Real-Time Monitoring Tool Administration Guide』

(<http://www.cisco.com/c/en/us/support/unified-communications/>)

[unified-communications-manager-callmanager/products-maintenance-guides-list.html](https://www.cisco.com/wwww/unified-communications-manager-callmanager/products-maintenance-guides-list.html)) を参照してください。

クレデンシャル キャッシングの設定

クレデンシャルキャッシングを有効にすると、システム効率が向上します。システムは、ログイン要求ごとに、データベースルックアップを実行したり、ストアードプロシージャを呼び出したりする必要がありません。キャッシュ期間が経過するまでは、関連付けられているクレデンシャルポリシーが適用されません。

この設定は、ユーザ認証を呼び出すすべての Java アプリケーションに適用されます。

手順

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

ステップ 2 必要に応じて、次のタスクを実行します。

- [キャッシングの有効化 (Enable Caching)] エンタープライズパラメータを [True] に設定します。このパラメータを有効にすると、Cisco Unified Communications Manager は、最大 2 分間、キャッシュされたクレデンシャルを使用します。
- システムがキャッシュされたクレデンシャルを認証に使用しないように、キャッシングを無効にするには、[キャッシングの有効化 (Enable Caching)] エンタープライズパラメータを [False] に設定します。LDAP 認証の場合、この設定は無視されます。クレデンシャルキャッシングでは、ユーザごとに最小量の追加メモリが必要です。

ステップ 3 [保存 (Save)] をクリックします。

セッションの終了の管理

管理者は、各ノードに固有のユーザのアクティブなサインインセッションを終了するために、次の手順を使用できます。



- (注)
- 特権レベル 4 を持つ管理者のみが、セッションを終了できます。
 - セッション管理では、特定のノード上のアクティブなサインインセッションを終了します。管理者は、異なるノード間ですべてのユーザセッションを終了する場合には、各ノードにサインインしてセッションを終了する必要があります。

これは、次のインターフェイスに適用されます。

- Cisco Unified CM Administration
- Cisco Unified Serviceability
- Cisco Unified Reporting
- Cisco Unified Communications セルフ ケア ポータル
- Cisco Unified CM IM and Presence の管理
- Cisco Unified IM and Presence サービスアビリティ
- Cisco Unified IM and Presence のレポート

手順

- ステップ 1** Cisco Unified OS Administration または Cisco Unified IM and Presence OS Administration から、[セキュリティ (Security)] > [セッション管理 (Session Management)] を選択します。
[セッション管理 (Session Management)] ウィンドウが表示されます。
- ステップ 2** [ユーザ ID (User ID)] フィールドにアクティブなサインイン ユーザのユーザ ID を入力します。
- ステップ 3** [セッションの終了 (Terminate Session)] をクリックします。
- ステップ 4** [OK] をクリックします。
-

終了したユーザは、サインインしたインターフェイスページを更新にすると、サインアウトします。監査ログにエントリが作成され、そこに終了した userID が表示されます。



第 VII 部

IPアドレス、ホスト名、およびドメイン名 の変更

- [変更前タスクとシステムヘルスチェック \(429 ページ\)](#)
- [IPアドレスおよびホスト名の変更 \(441 ページ\)](#)
- [ドメイン名およびノード名の変更 \(451 ページ\)](#)
- [変更後のタスクと検証 \(465 ページ\)](#)
- [アドレス変更に関する問題のトラブルシューティング \(475 ページ\)](#)



第 29 章

変更前タスクとシステムヘルスチェック

- [変更前のタスク](#) (429 ページ)
- [IP アドレス、ホスト名、およびその他のネットワーク識別子の変更](#) (429 ページ)
- [手順のワークフロー](#) (432 ページ)
- [Cisco Unified Communications Manager ノードの変更前タスク](#) (434 ページ)
- [IM and Presence サービス ノードの変更前セットアップタスク](#) (436 ページ)

変更前のタスク

IP アドレス、ホスト名、およびその他のネットワーク識別子の変更

導入におけるノードのネットワークレベルの IP アドレスとホスト名をさまざまな理由で変更できます。これには、クラスタ間でノードを移動することや、重複している IP アドレスの問題を解決することが含まれます。IP アドレスは、ノードに関連付けられたネットワークレベルの Internet Protocol (IP) ではホスト名は、ノードのネットワークレベルのホスト名です。



(注) すべての統合コミュニケーション製品 (Cisco Unified Communications Manager、Cisco Unity Connections、シスコ IM and Presence など) は、1つのインターフェイスしか持っていません。したがって、これらの製品ごとに IP アドレスを 1 つずつ割り当てることができます。

ノード名やドメイン名など、その他のネットワーク ID の変更については、次のリソースを参照してください。

- [Cisco Unified Communications Manager システム設定ガイド](#)
- [IM and Presence Service 設定および管理ガイド](#)
- 『[Installation Guide for Cisco Unified Communications Manager and the IM and Presence Service](#)』

IM and Presence Serviceにおけるノードのノード名およびネットワーク レベル DNS デフォルトドメイン名を変更する手順については、このドキュメントでも扱われています。

IM and Presence Service ノード名およびデフォルトのドメイン名の変更

ノード名は、Cisco Unified CM Administration GUI を使用して設定され、その他すべての IM and Presence Service ノードとすべてのクライアント マシンから解決可能である必要があります。したがって、推奨されるノード名の値は、ノードのネットワーク FQDN です。ただし、IP アドレスとホスト名のどちらも、特定の導入ではノード名の値としてサポートされています。ノード名 **ホスト名の設定 (323 ページ)** の推奨事項とサポートされている導入タイプの詳細については、を参照してください。

ノードのネットワーク レベルの DNS デフォルト ドメイン名はホスト名と結合され、ノードの完全修飾ドメイン名 (FQDN) を形成します。たとえば、ホスト名が「imp-server」で、ドメインが「example.com」であるノードの FQDN は「imp-server.example.com」になります。

ノードのネットワーク レベル DNS デフォルト ドメインを、IM and Presence Service アプリケーションの企業ドメインと混同しないでください。

- ネットワークレベルの DNS デフォルト ドメインは、ノードのネットワーク ID としてのみ使用されます。
- 企業の IM and Presence Service ドメインは、エンドユーザの IM アドレスで使用されるアプリケーション レベルのドメインです。

Cisco Unified CM IM and Presence Administration GUI または Cisco Unified Communications Manager Administration を使用して企業全体のドメインを設定できます。企業ドメインの推奨事項とサポートされる導入タイプの詳細については、『*Deployment Guide for IM and Presence Service on Cisco Unified Communications Manager*』を参照してください。

ホスト名の設定

次の表に、Unified Communications Manager サーバのホスト名を設定できる場所、ホスト名として指定できる文字数、および推奨されるホスト名の先頭文字と最終文字を示します。ホスト名を正しく設定しないと、Unified Communications Manager の一部のコンポーネント（オペレーティングシステム、データベース、インストールなど）が期待通りに機能しない可能性があります。

表 82: Cisco Unified Communications Manager におけるホスト名の設定

ホスト名の場所	可能な設定	指定できる文字数	推奨されるホスト名の先頭文字	推奨されるホスト名の最終文字
[ホスト名/IP アドレス (Host Name/IP Address)] フィールド Cisco Unified Communications Manager Administration の [システム (System)] > [サーバ (Server)]	クラスタ内のサーバのホスト名を追加または変更できません。	2 ~ 63	英字	英数字
[ホスト名 (Hostname)] フィールド Cisco Unified Communications Manager インストール ウィザード	クラスタ内のサーバのホスト名を追加できます。	1 ~ 63	英字	英数字
[ホスト名 (Hostname)] フィールド Cisco Unified Communications オペレーティング システム の [設定 (Settings)] > [IP] > [イーサネット (Ethernet)]	クラスタ内のサーバのホスト名を変更できますが、追加はできません。	1 ~ 63	英字	英数字
set network hostname hostname コマンドライン インターフェイス	クラスタ内のサーバのホスト名を変更できますが、追加はできません。	1 ~ 63	英字	英数字



ヒント このホスト名は、ARPANET ホスト名の規則に従う必要があります。ホスト名の先頭文字と最終文字の間には、英数文字とハイフンを入力できます。

いずれかの場所でホスト名を設定する前に、次の情報を確認してください。

- [サーバの設定 (Server Configuration)] ウィンドウの [ホスト名/IP アドレス (Host Name/IP Address)] フィールドは、デバイスとサーバ間、アプリケーションとサーバ間、および異なるサーバ間の通信をサポートします。このフィールドには、ドット区切り形式の IPv4 アドレスまたはホスト名を入力できます。

Unified Communications Manager パブリッシャ ノードをインストールした後は、パブリッシャのホスト名がこのフィールドに自動的に表示されます。Unified Communications Manager サブスクライバ ノードをインストールする前に、Unified Communications Manager パブリッシャ ノードでこのフィールドにサブスクライバ ノードの IP アドレスまたはホスト名を入力してください。

このフィールドにホスト名を設定できるのは、Unified Communications Manager が DNS サーバにアクセスしてホスト名を IP アドレスに解決できる場合のみです。DNS サーバに Cisco Unified Communications Manager の名前とアドレスの情報が設定されていることを確認してください。



ヒント DNS サーバに Unified Communications Manager の情報を設定するのに加えて、Cisco Unified Communications Manager のインストール時に DNS 情報を入力します。

- Unified Communications Manager パブリッシャ ノードのインストール時に、ネットワーク情報を設定するために（つまり、スタティック ネットワークを使用する場合に）パブリッシャ サーバのホスト名（必須）と IP アドレスを入力します。

Unified Communications Manager サブスクリバ ノードのインストール時には、Unified Communications Manager パブリッシャ ノードのホスト名と IP アドレスを入力して、Unified Communications Manager がネットワークの接続性およびパブリッシャ とサブスクリバ 間の検証を確認できるようにしてください。さらに、サブスクリバ ノードのホスト名と IP アドレスも入力する必要があります。Unified Communications Manager のインストール時にサブスクリバ サーバのホスト名の入力を求められた場合は、Cisco Unified Communications Manager Administration の [ホスト名/IP アドレス (Host Name/IP Address)] フィールドでサブスクリバ サーバのホスト名を設定した場合に [サーバの設定 (Server Configuration)] ウィンドウに表示される値を入力します。

手順のワークフロー

Cisco Unified Communications Manager ワークフロー

このドキュメントでは、Cisco Unified Communications Manager ノード上における次のタスクの詳細な手順を取り上げます。

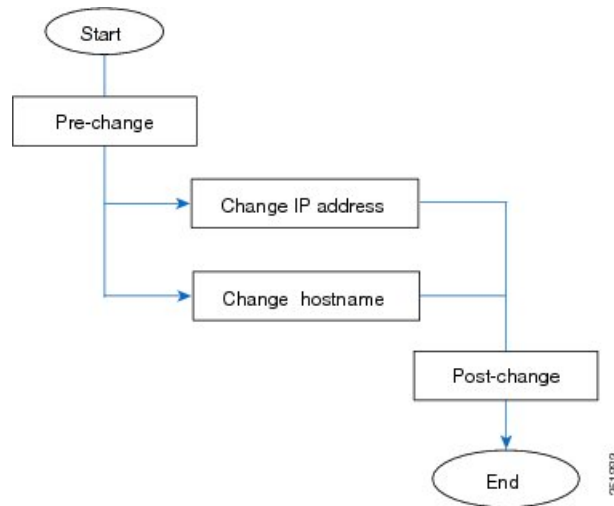
- ノードの IP アドレスの変更
- ノードのホスト名の変更

実行するステップを要約したそれぞれの手順に関してタスク リストが示されます。



(注) こうした変更を行う前に変更前タスクすべてとシステムヘルスチェックを実行し、変更後には変更後タスクを実行しなければなりません。

図 24 : Cisco Unified Communications Manager ワークフロー



3511882

IM and Presence Service のワークフロー

このマニュアルでは、IM and Presence Service ノードに対する以下の作業の詳細な手順を示します。

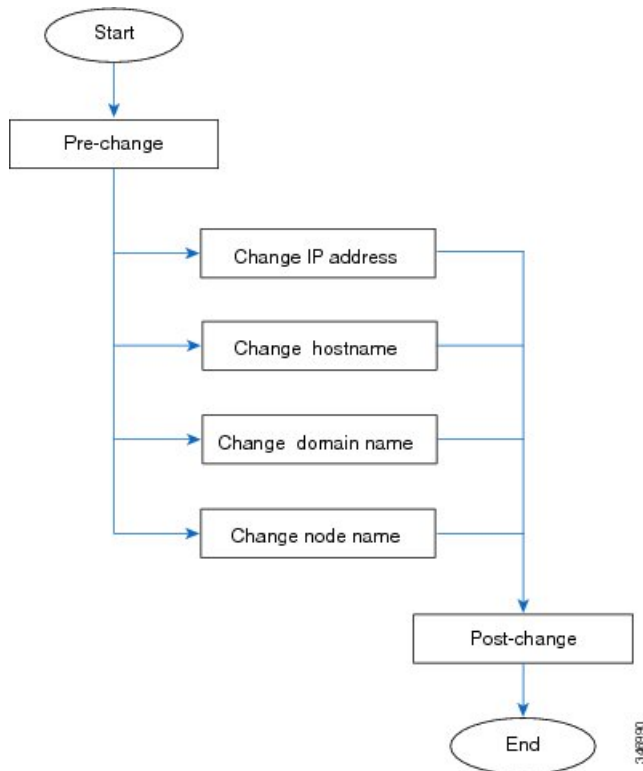
- ノードの IP アドレスの変更
- ノードのホスト名の変更
- DNS デフォルト ドメイン名の変更
- ノードのノード名の変更

実行するステップを要約したそれぞれの手順に関してタスク リストが示されます。



(注) こうした変更を行う前に変更前タスクすべてとシステムヘルスチェックを実行し、変更後には変更後タスクを実行しなければなりません。

図 25: IM and Presence Service のワークフロー



Cisco Unified Communications Manager ノードの変更前タスク

次の手順では、Cisco Unified Communications Manager ノードの IP アドレスとホスト名を変更するタスクについて説明します。これらの手順は、スケジュールしたメンテナンス時間内に実行する必要があります。



注意 これらのタスクを実行しても期待する結果が得られない場合は、問題が解決されるまで続行しないでください。

手順

- ステップ 1** Cisco Unified Communications Manager サーバ内で DNS が設定されている場合、正引きおよび逆レコード (A レコードと PTR レコードなど) が設定されていて、DNS が到達可能で作動していることを確認します。

ステップ 2 アクティブな **ServerDown** 警告が出ていないことを確認し、クラスタ内のすべてのサーバが稼働していて利用可能であることを確かめます。最初のノードで、Cisco Unified Real-Time Monitoring Tool (RTMT) またはコマンドラインインターフェイス (CLI) のいずれかを使用します。

- a) Unified RTMT を使用して確認するには、Alert Central にアクセスし、ServerDown 警告が発生していないか調べます。
- b) 最初のノードで CLI を使用して確認するには、次の CLI コマンドを入力してアプリケーションのイベント ログを調べます。

```
file search activelog syslog/CiscoSyslog ServerDown
```

出力例については、データベースレプリケーションの出力例に関するトピックを参照してください。詳細な手順およびトラブルシューティングについては、データベースレプリケーションおよびデータベースレプリケーションのトラブルシューティングについてのトピックを参照してください。

ステップ 3 クラスタにあるすべての Cisco Unified Communications Manager ノードでデータベースレプリケーションのステータスを調べ、すべてのサーバがデータベースの変更内容を正常に複製していることを確認します。IM and Presence Service の場合、導入環境に複数のノードがあるときにはデータベースパブリッシャ ノードでデータベースレプリケーションのステータスを調べます。Unified RTMT または CLI を使用します。すべてのノードで 2 のステータスが表示される必要があります。

1. RTMT を使用して確認するには、Database Summary にアクセスしてレプリケーションのステータスを調べます。
2. CLI を使用して確認するには、**utils dbreplication runtimestate** と入力します。

ステップ 4 次の例に示されているように CLI コマンド **utils diagnose** を入力し、ネットワーク接続と DNS サーバの設定を確認してください。

例 :

```
admin: utils diagnose module validate_network
Log file: /var/log/active/platform/log/diag1.log
Starting diagnostic test(s)
=====
test - validate_network : Passed
Diagnostics Completed
admin:
```

ステップ 5 Cisco Unified レポート ツールで **Unified CM Database Status** レポートを生成します。そのレポートにエラーや警告が記録されていないか確認します。

ステップ 6 Cisco Unified レポート ツールで **Unified CM Cluster Overview** レポートを生成します。そのレポートにエラーや警告が記録されていないか確認します。

ステップ 7 最初のノードの Cisco Unified Communications Manager Administration から、[システム (System)] > [サーバ (Server)] の順に選択し、[検索 (Find)] をクリックします。クラスタにあるすべてのサーバが一覧表示されます。後で参照できるように、サーバのこのリストを保持します。ク

ラスト内のノードごとに、ホスト名と IP アドレスの両方のインベントリが保存されていることを確認します。

- ステップ 8** 手動でディザスタ リカバリ システムのバック アップを実行し、すべてのノードとアクティブなサービスが正しくバック アップされていることを確認します。詳細については、『*Administration Guide for Cisco Unified Communications Manager*』を参照してください。
- ステップ 9** ホスト名を変更する場合、SAML シングルサインオン (SSO) を無効にします。SAML SSO の詳細については、『*Deployment Guide for IM and Presence Service on Cisco Unified Communications Manager*』を参照してください。
- ステップ 10** セキュリティが有効なクラスタ (クラスタセキュリティ モード 1-混合) について、証明書信頼リスト (CTL) ファイルを更新します。既存の CTL ファイルへの新しい TFTP サーバの追加など、CTL ファイルの更新と管理の方法の詳細については、『*Cisco Unified Communications Manager Security Guide*』を参照してください。

(注) 通信不可能な時間が無駄に発生しないように、TFTP サーバの新しい IP アドレスで CTL ファイルを更新してから、TFTP サーバの IP アドレスを変更するようにします。この手順を実行しない場合は、セキュリティが有効なすべての IP 電話を手動で更新する必要があります。

(注) セキュリティをサポートしているすべての IP 電話では、CTL ファイルが必ずダウンロードされます。このファイルには、その電話からの通信が許可されている TFTP サーバの IP アドレスが記述されています。TFTP サーバの IP アドレスを変更した場合は、その新しい IP アドレスを CTL ファイルに追加する必要があります。これにより、該当の電話からその TFTP サーバと通信できるようになります。

IM and Presence サービス ノードの変更前セットアップタスク

該当する変更前セットアップタスクを実行して IP アドレス、ホスト名、ドメイン、またはノード名が正常に変更されるようにシステムが準備されていることを確認します。これらのタスクは、スケジュールしたメンテナンス時間内に実行する必要があります。



注意 これらのタスクを実行しても期待する結果が得られない場合は、問題が解決されるまで続行しないでください。



(注) ドメイン名またはノード名を変更しない限り、Cisco AXL Web サービス、および IM and Presence Cisco Sync Agent サービスが起動していることを確認する手順を実行する必要はありません。実行するタスクの完全な一覧については、変更前のタスク リストを参照してください。

手順

ステップ 1 クラスタにあるすべてのノードでデータベースレプリケーションのステータスを調べ、すべてのサーバがデータベースの変更内容を正常に複製していることを確認します。

IM and Presence Service の場合、導入環境に複数のノードがあるときにはデータベースパブリッシャノードでデータベースレプリケーションのステータスを調べます。

Unified RTMT または CLI を使用します。すべてのノードで **2** のステータスが表示される必要があります。

- a) RTMT を使用して確認するには、Database Summary にアクセスしてレプリケーションのステータスを調べます。
- b) CLI を使用して確認するには、`utils dbreplication runtimestate` を入力します。
出力例については、データベースレプリケーションの出力例に関するトピックを参照してください。詳細な手順およびトラブルシューティングについては、データベースレプリケーションおよびデータベースレプリケーションのトラブルシューティングについてのトピックを参照してください。

ステップ 2 次の例に示されているように CLI コマンド `utils diagnose` を入力し、ネットワーク接続と DNS サーバの設定を確認してください。

例：

```
admin: utils diagnose module validate_network Log file:
/var/log/active/platform/log/diag1.log Starting diagnostic test(s)
===== test - validate_network : Passed Diagnostics
Completed admin:
```

ステップ 3 手動でディザスタリカバリシステムのバックアップを実行し、すべてのノードとアクティブなサービスが正しくバックアップされていることを確認します。

詳細については、『*Administration Guide for Cisco Unified Communications Manager*』を参照してください。

ステップ 4 すべてのプレゼンス冗長グループでハイアベイラビリティ (HA) を無効にします。プレゼンス冗長グループの構成情報は、*Cisco Unified Communications Manager* システム設定ガイドの「プレゼンス冗長グループの設定」の章を参考してください。

- (注)
- HA を無効にする前に、各ノードとサブクラスタのユーザ数の記録を取ります。この情報は、[Cisco Unified CM IM and Presence の管理 (Cisco Unified CM IM and Presence Administration)] の [システム (System)] > [プレゼンス トポロジ (Presence Topology)] ウィンドウで見つけることができます。
 - HA を無効にした後、さらに変更を完了する前に、クラスタ全体で設定が同期されるまで少なくとも2分間待機します。

- ステップ 5** ホスト名を変更する場合、SAML シングルサインオン (SSO) を無効にします。SAML SSO の詳細については、『*Deployment Guide for IM and Presence Service on Cisco Unified Communications Manager*』を参照してください。
- ステップ 6** 現在アクティブなすべてのサービスのリストをまとめます。後で参照できるように、これらのリストを保持します。
- Cisco Unified Serviceability を使用してアクティブなネットワーク サービスのリストを表示するには、[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。
 - Cisco Unified Serviceability を使用してアクティブな機能サービスのリストを表示するには、[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 7** Cisco Unified Serviceability を使用してすべての機能サービスを停止するには、[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。機能サービスを停止する順序は重要ではありません。
- ヒント** IP アドレス、ホスト名、または IP アドレスとホスト名の両方を変更する場合、この手順を実行する必要はありません。これらの名前の変更に対して、機能サービスは自動的に停止します。
- ステップ 8** [ツール (Tools)] > [コントロール センター機能サービス (Control Center - Services)] を選択するときに、Cisco Unified Serviceability を使用して [IM and Presence サービス (IM and Presence Service)] サービスグループの下にリストされる以下のネットワークサービスを停止します。次の順序で、これらの IM and Presence Service ネットワーク サービスを停止する必要があります。
- Cisco Config Agent
 - Cisco Intercluster Sync Agent
 - Cisco Client Profile Agent
 - Cisco OAM Agent
 - Cisco XCP Config Manager
 - Cisco XCP Router
 - Cisco Presence Datastore
 - Cisco SIP Registration Datastore
 - Cisco Login Datastore
 - Cisco Route Datastore
 - Cisco Server Recovery Manager
 - Cisco IM and Presence Data Monitor
- ステップ 9** Cisco Unified 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)]) を使用して、Cisco AXL Web Service が Cisco Unified Communications Manager パブリッシュャ ノードで起動していることを確認します。
- (注) ドメイン名またはノード名を変更する場合にのみ、この手順を実行します。
- ステップ 10** IM and Presence Cisco Sync Agent サービスが開始し、同期が完了したことを確認します。

(注) ドメイン名またはノード名を変更する場合にのみ、この手順を実行します。

- a) Cisco Unified Serviceability を使用して確認するには、以下の手順を実行します。
1. [ツール (Tools)] > [コントロールセンターのネットワーク サービス (Control Center - Network Services)] を選択します。
 2. IM and Presence データベース パブリッシャ ノードを選択します。
 3. [IM and Presence サービス (IM and Presence Service)] サービスを選択します。
 4. Cisco Sync Agent サービスが開始していることを確認します。
 5. Cisco Unified CM IM and Presence Administration GUI から、[診断 (Diagnostics)] > [システム ダッシュボード (System Dashboard)] > [同期ステータス (Sync Status)] を選択します。
 6. 同期が完了し、同期ステータス領域にエラーが表示されていないことを確認します。
- b) IM and Presence データベース パブリッシャ ノードで Cisco Unified CM IM and Presence Administration GUI を使用して確認するには、[診断 (Diagnostics)] > [システム ダッシュボード (System Dashboard)] を選択します。
-



第 30 章

IP アドレスおよびホスト名の変更

- IP アドレスとホスト名の変更のタスク リスト (441 ページ)
- OS Admin GUI による IP アドレスまたはホスト名の変更 (442 ページ)
- Unified CM の管理 GUI による IP アドレスまたはホスト名の変更 (443 ページ)
- CLI による IP アドレスまたはホスト名の変更 (444 ページ)
- IP アドレスのみの変更 (447 ページ)
- CLI による IP アドレスまたはホスト名の変更 (448 ページ)

IP アドレスとホスト名の変更のタスク リスト

次の表に、Cisco Unified Communications Manager と IM and Presence Service ノードの IP アドレスとホスト名を変更するために実行するタスクを示します。

表 83: IP アドレスとホスト名の変更のタスク リスト

項目	タスク
1	変更前タスクおよびシステム ヘルス チェックを行います。
2	<p>コマンドライン インターフェイス (CLI) または Unified オペレーティング システム GUI を使用してノードの IP アドレスまたはホスト名を変更します。</p> <p>IM and Presence Service ノードの場合、次の条件に従ってください。</p> <ul style="list-style-type: none">• サブスクライバ ノードを変更する前にデータベース パブリッシャ ノードの IP アドレスとホスト名を変更します。• すべてのサブスクライバ ノードの IP アドレスとホスト名を同時に変更する、もしくは、一度に 1 つずつ変更することが可能です。 <p>(注) IM and Presence Service ノードの IP アドレスまたはホスト名を変更した後、Cisco Unified Communications Manager の SIP パブリッシュ トランクの接続先アドレス値を変更する必要があります。変更後タスク リストを参照してください。</p>

項目	タスク
3	変更後タスクを実行します。

OS Admin GUI による IP アドレスまたはホスト名の変更

Cisco Unified Operating System Administration を使用して、導入のホスト名で定義されているパブリッシャーおよびサブスクリバノードの IP アドレスまたはホスト名を変更することができます。特に明記されていない限り、この手順の各ステップは、Unified Communications Manager および IM and Presence Service クラスタ上のパブリッシャーノードとサブスクリバノードの両方に適用されます。

set network hostname コマンドでホスト名を変更すると、自己署名証明書が自動的に再生成されます。これにより、クラスタ内のすべてのデバイスがリセットされ、更新された ITL ファイルをダウンロードできるようになります。クラスタが CA 署名付き証明書を使用する場合は、証明書に再署名する必要があります。

set network hostname コマンドを使用して IP アドレスのみを変更すると、クラスタ内のすべてのデバイスがリセットされ、更新された ITL ファイルをダウンロードできるようになります。証明書は更新されません。



(注) ホスト名を変更しても、ITL 回復証明書の再生成はトリガーされません。



注意

- Cisco ユニファイドオペレーティングシステムの管理では、これらの設定の1つだけを一度に変更することをお勧めします。IP アドレスとホスト名の両方を同時に変更するには、CLI コマンド **set network hostname** を使用します。
- Unified Communications Manager のセキュリティクラスタが混合モードで実行されている場合にホスト名または IP アドレスを変更すると、このノードへのセキュア接続は、CTL クライアントを実行して CTL ファイルを更新しない限り（またはトークンレス CTL 機能を使用している場合は **utils ctl update CTLFile** を実行しない限り）失敗します。

始める前に

導入環境で変更前タスクとシステムヘルスチェックを実行します。



(注) vcenter から vNIC を変更する必要がある場合は、CLI コマンド **set network hostname** を使用する必要があります。

手順

ステップ 1 Cisco Unified Operating System Administration から、[設定 (Settings)] > [IP] > [イーサネット (Ethernet)] の順に選択します。

ステップ 2 ホスト名、IP アドレス、また必要に応じてデフォルトのゲートウェイを変更します。

ステップ 3 [保存 (Save)] をクリックします。

ノードサービスが新しい変更内容で自動的に再起動します。サービスを再起動することで、更新とサービス再起動のシーケンスを適切に実行して、変更を有効にすることができます。

ホスト名を変更すると、自己署名証明書が自動的に再生成されます。また、更新された ITL ファイルをダウンロードできるように、クラスタ内のすべてのデバイスがリセットされます。ホスト名を変更しても、ITL 回復証明書の再生成はトリガーされません。

次のタスク

導入の変更が正しく実行されていることを確認するすべての該当する変更後の作業を実行します。



(注) 新しいホスト名が正しい IP アドレスに解決されない場合は、次の手順に進まないでください。

クラスタが CA 署名付き証明書を使用する場合は、証明書に再署名する必要があります。

CTL クライアントを実行して、そのプロセスを使用してクラスタを混合モードにする場合は、ctl ファイルを更新します。トークンレス CTL 機能を使用した場合は、CLI コマンドユーティリティの `ctl Update CTLFile` を実行します。

Unified CM の管理 GUI による IP アドレスまたはホスト名の変更

Cisco Unified CM Administration を使用して、パブリッシャおよびサブスクライバノードのデータベースで定義された IP アドレスまたはホスト名を変更することができます。これにより、ホスト名のエントリがシステム定義のホスト名または IP 値で統一されます。

IP アドレスまたはホスト名を変更すると、自己署名証明書が自動的に再生成されます。これにより、クラスタ内のすべてのデバイスがリセットされ、更新された ITL ファイルをダウンロードできるようになります。クラスタが CA 署名付き証明書を使用する場合は、証明書に再署名する必要があります。

**注意**

- ホスト名または IP アドレスを変更すると、システムサービスを再起動する必要があります。したがって、通常の営業時間中にはこの変更を行わないでください。
- Cisco Unified CM の管理では、これらの設定の1つだけを一度に変更することをお勧めします。IP アドレスとホスト名の両方を同時に変更するには、CLI コマンド **set network hostname** を使用します。
- Unified Communications Manager のセキュリティ クラスタが混合モードで実行されている場合にホスト名または IP アドレスを変更すると、このノードへのセキュア接続は、CTL クライアントを実行して CTL ファイルを更新しない限り（またはトークンレス CTL 機能を使用している場合は **utils ctl update CTLFile** を実行しない限り）失敗します。
- Cisco Unified OS の管理ページと Cisco Unified CM の管理ページで定義されているホスト名または IP アドレスが一致しない場合、アプリケーションは正しい電話ステータスを取得できません。また、証明書の不一致により、TLS ハンドシェイクが失敗します。したがって、Cisco Unified OS の管理ページと Cisco Unified CM の管理ページの両方の IP アドレスとホスト名のエントリが同じであることを確認してください。

始める前に

導入環境で変更前タスクとシステムヘルスチェックを実行します。

手順

- ステップ 1** Cisco Unified CM の管理から、[システム (System)] > [サーバ (Server)] を選択します。
[サーバの検索/一覧表示 (Find and List Servers)] ウィンドウが表示されます。
- ステップ 2** すべてのサーバのリストを取得するには、[検索 (Find)] をクリックします。
- ステップ 3** リストから、ホスト名を変更するサーバをクリックします。
- ステップ 4** [ホスト名/IP アドレス* (Host Name/IP Address*)] フィールドに、ネットワーク サーバのホスト名または IP アドレスを入力し、[保存 (Save)] をクリックします。
- ステップ 5** Admin CLI GUI を使用して、**utils system restart CLI** コマンドを使用してノードを再起動します。

CLI による IP アドレスまたはホスト名の変更

導入のホスト名で定義されているパブリッシャおよびサブスクリバノードの IP アドレスまたはホスト名を変更するには、CLI を使用できます。特に明記されていない限り、この手順の各ステップは、Cisco Unified Communications Manager と IM and Presence Service クラスタのパブリッシャノードとサブスクリバノードの両方に適用されます。

ホスト名を変更すると、自己署名証明書が自動的に再生成されます。これにより、クラスタ内のすべてのデバイスがリセットされ、更新されたITLファイルをダウンロードできるようになります。クラスタが CA 署名付き証明書を使用する場合は、証明書に再署名する必要があります。ホスト名を変更しても、ITL 回復証明書の再生成はトリガーされません。



注意 Cisco Unified Communications Manager のセキュリティ クラスタが混合モードで実行されている場合にホスト名または IP アドレスを変更すると、このノードへのセキュア接続は、CTL クライアントを実行して CTL ファイルを更新しない限り（またはトークンレス CTL 機能を使用している場合は **utils ctl update CTLFile** を実行しない限り）失敗します。



(注) Unified Communications Manager およびインスタント メッセージおよびプレゼンスサーバで IP / ドメイン/ホスト名を変更するプロセス中の障害を回避するために、COP ファイルをインストールする必要があります。

始める前に

導入環境で変更前タスクとシステムヘルスチェックを実行します。

手順

- ステップ 1** 変更するノードの CLI にログインします。
- ステップ 2** **set network hostname** と入力します。
- ステップ 3** ホスト名、IP アドレス、またはデフォルト ゲートウェイを変更するためのプロンプトに従います。
 - a) 新しいホスト名を入力し、**Enter** キーを押します。
 - b) IP アドレスも変更する場合は、**yes** と入力します。その他の場合は、ステップ 4 に進みます。
 - c) 新しい IP アドレスを入力します。
 - d) サブネットマスクを入力します。
 - e) ゲートウェイのアドレスを入力します。
- ステップ 4** 入力内容がすべて正しいことを確認し、**yes** と入力して、プロセスを開始します。

次のタスク

導入の変更が正しく実行されていることを確認するすべての該当する変更後の作業を実行します。



(注) 新しいホスト名が正しい IP アドレスに解決されない場合は、次の手順に進まないでください。

クラスタが CA 署名付き証明書を使用する場合は、証明書に再署名する必要があります。

CTL クライアントを実行して、そのプロセスを使用してクラスタを混合モードにする場合は、ctl ファイルを更新します。トークンレス CTL 機能を使用した場合は、CLI コマンドユーティリティの `ctl Update CTLFile` を実行します。

Set Network Hostname の CLI 出力例



(注) vNIC を vcenter から変更する必要がある場合は、次の出力に示すように、ステップ 4/5 のコンポーネント通知スクリプト `regenerate_all_certs.sh` の後に vNIC を更新します。

```
admin:set network hostname ctrl-c: To quit the input. *** W A R N I N G ***
Do not close this window without first canceling the command. This command will
automatically restart system services. The command should not be issued during
normal operating hours. =====
Note: Please verify that the new hostname is a unique name across the cluster
and, if DNS services are utilized, any DNS configuration is completed before
proceeding. ===== Security
Warning : This operation will regenerate all CUCM Certificates including any
third party signed Certificates that have been uploaded. Enter the hostname::
newHostname Would you like to change the network ip address at this time
[yes]:: Warning: Do not close this window until command finishes. ctrl-c: To
quit the input. *** W A R N I N G ***
===== Note: Please verify
that the new ip address is unique across the cluster.
===== Enter the ip address::
10.10.10.28 Enter the ip subnet mask:: 255.255.255.0 Enter the ip address of
the gateway:: 10.10.10.1 Hostname: newHostname IP Address: 10.10.10.28 IP
Subnet Mask: 255.255.255.0 Gateway: 10.10.10.1 Do you want to continue [yes/no]?
yes calling 1 of 5 component notification script: ahostname_callback.sh Info(0):
Processnode query returned = name ===== bldr-vcml8 updating server table
from:'oldHostname', to: 'newHostname' Rows: 1 updating database, please wait
90 seconds updating database, please wait 60 seconds updating database, please
wait 30 seconds Going to trigger /usr/local/cm/bin/dbl updatefiles
--remote=newHostname,oldHostname calling 2 of 5 component notification script:
clm_notify_hostname.sh notification Verifying update across cluster nodes...
platformConfig.xml is up-to-date: bldr-vcml21 cluster update successfull calling
3 of 5 component notification script: drf_notify_hostname_change.py calling
4 of 5 component notification script: regenerate_all_certs.sh calling 5 of 5
component notification script: update_idsendv.sh calling 1 of 2 component
notification script: ahostname_callback.sh Info(0): Processnode query returned
= name ==== Going to trigger /usr/local/cm/bin/dbl updatefiles
--remote=10.10.10.28,10.67.142.24 calling 2 of 2 component notification script:
clm_notify_hostname.sh Verifying update across cluster nodes... Shutting down
interface eth0:
```

IP アドレスのみの変更

CLI を使用して、ノードの IP アドレスを変更できます。

ノードがホスト名または FQDN によって定義されている場合は、変更を行う前に DNS のみを更新する必要があります (DNS が使用されている場合)。



(注) IM and Presence Service の場合 :

- 最初に IM and Presence データベース パブリッシャ ノードを変更して確認します。
- IM and Presence Service サブスクリバ ノードは、同時にまたは 1 つずつ変更できます。

始める前に

導入環境で変更前タスクとシステムヘルスチェックを実行します。

手順

ステップ 1 変更するノードの CLI にログインします。

ステップ 2 `set network ip eth0 new-ip_address new_netmask new_gateway` を入力して、ノードの IP アドレスを変更します。

(注) `set network ip eth0` コマンドでのみ IP アドレスを変更しても、証明書の再生成はトリガーされません。

ここで、`new_ip_address` は新しいサーバ IP アドレスを指定し、`new_netmask` は新しいサーバネットワーク マスクを指定します。また、`new_gateway` はゲートウェイアドレスを指定します。

次の出力が表示されます。

```
admin:set network ip eth0 10.53.57.101 255.255.255.224 10.53.56.1 WARNING:
Changing this setting will invalidate software license on this server. ライセン
スは再ホストする必要があります。Continue (y/n)?
```

ステップ 3 CLI コマンドの出力を確認します。 **yes** を入力してから、**Enter** を押して処理を開始します。

次のタスク

導入の変更が正しく実行されていることを確認するすべての該当する変更後の作業を実行します。

ネットワーク IP アドレスの設定の出力例



Note vNIC を vcenter から変更する必要がある場合は、次の出力に示すように、ステップ 3/6 のコンポーネント通知スクリプト `aetc_hosts_verify.sh` の後に vNIC を更新します。

```
admin:set network ip eth0 10.77.30.34 255.255.255.0 10.77.30.1 *** W A R N I
N G *** This command will restart system services
===== Note: Please verify
that the new ip address is unique across the cluster and, if DNS services are
utilized, any DNS configuration is completed before proceeding.
===== Continue (y/n)?y calling
1 of 6 component notification script: acluster_healthcheck.sh calling 2 of 6
component notification script: adns_verify.sh No Primary DNS server defined
No Secondary DNS server defined calling 3 of 6 component notification script:
aetc_hosts_verify.sh calling 4 of 6 component notification script: afupdateip.sh
calling 5 of 6 component notification script: ahostname_callback.sh Info(0):
Processnode query returned using 10.77.30.33: name ==== calling 6 of 6 component
notification script: clm_notify_hostname.sh
```

CLI による IP アドレスまたはホスト名の変更

CLI を使用して、展開内のパブリッシャ ノードとサブスクライバノードの DNS IP アドレスを変更することができます。この手順は、Unified Communications Manager のパブリッシャ ノードとサブスクライバノード、および IM and Presence サービスクラスタの両方に適用されます。



(注) DNS サーバーレコードのいずれかに変更がある場合、または DNS サーバー自体に変更がある場合、ユーザは `nscd` サービスを再起動する必要があります。この再起動により、キャッシュレコードがクリアされ、新しいレコードがキャッシュにロードされます。

始める前に

導入環境で変更前タスクとシステムヘルスチェックを実行します。

手順

ステップ 1 変更するノードの CLI にログインします。

ステップ 2 `set network dns primary/secondary <new IP address of the DNS>` と入力します。

(注) DNS サーバの IP アドレスを変更する場合は、ユーティリティシステム再起動 CLI コマンドを使用してサーバを再起動する必要があります。

以下の出力が表示されます。


```
admin:set network dns primary/secondary <new IP address of DNS> *** W A R N I  
N G *** This will cause the system to temporarily lose network connectivity
```

ステップ 3 CLI コマンドの出力を確認します。はいを入力して、**Enter** キーを押して処理を開始します。



第 31 章

ドメイン名およびノード名の変更

- [ドメイン名の変更 \(451 ページ\)](#)
- [ノード名の変更 \(459 ページ\)](#)
- [Cisco Unified Communications Manager のドメイン名の更新 \(463 ページ\)](#)

ドメイン名の変更

管理者は、IM and Presence Service ノードまたはノードグループに関連付けられたネットワークレベルの DNS デフォルト ドメインを変更できます。

企業全体の IM and Presence Service ドメインは、IM and Presence Service ノードの DNS デフォルトドメインと対応している必要はありません。展開のために企業全体のドメインを変更するには、IM and Presence サービスの『*deployment guide for IM and Presence service on Cisco Unified Communications Manager Configuration and Administration guide*』を参照してください。



注意 IM and Presence Service クラスタ内のノードのデフォルト ドメインを変更すると、ノードが再起動し、プレゼンスサービスやその他のシステム機能が中断されます。システムにこのような影響があることから、このドメイン変更手順は、スケジュールしたメンテナンス時間の中で実行する必要があります。

ノードのデフォルト ドメイン名を変更すると、すべてのサードパーティの署名済みセキュリティ証明書が新しい自己署名証明書によって自動的に上書きされます。これらの証明書をサードパーティの認証局によって再署名するには、新しい証明書を手動で要求してアップロードする必要があります。こうした新しい証明書を有効にするには、サービスの再起動が必要になることがあります。新しい証明書の要求に要する時間によっては、メンテナンス時間を別途設定して、サービスの再起動スケジュールを設定することが必要になる場合もあります。



(注) ノードのデフォルト ドメイン名を変更する前に、新しい証明書を要求することはできません。証明書署名要求 (CSR) の生成は、ノードでドメインを変更し、そのノードを再起動した後のみ可能です。

IM and Presence サービスのデフォルト ドメイン名の変更作業

次の表に、IM and Presence Service ノードまたはノード グループに関連付けられたネットワーク レベル DNS デフォルト ドメイン名を変更するためのステップごとの手順を示します。この手順の詳しい説明では、クラスタにある複数のノードに対する変更を実行するステップの正確な順序を指定しています。

複数のクラスタにわたってこの手順を実行する場合は、順番に一度に1つのクラスタで変更を完了する必要があります。



(注) この手順の各タスクは、この表に示された順序どおりに実行する必要があります。

手順

ステップ 1 クラスタ内のすべての該当するノードで変更前の作業を完了します。変更前の作業の一部は IM and Presence データベース パブリッシャ ノードだけに適用し、サブスクリバ ノードを変更する場合はスキップすることができます。

ステップ 2 クラスタ内のすべての該当するノードで、IM and Presence Service ノードの DNS レコードを更新します。SRV、順方向 (A)、および逆方向 (PTR) の各レコードも必要に応じて更新し、新しいノード ドメインを取り入れます。

ステップ 3 Cisco Unified Communications Manager Administration を使用して、クラスタ内のすべての該当するノードで、IM and Presence Service ノード名を更新します。

(注) この手順は FQDN ノード名の形式に必須です。ノード名が IP アドレスまたはホスト名の場合は適用されません。

- ノード名が FQDN であるノードでは、ドメイン変更前のノードのドメイン名を参照しています。したがって、FQDN の値に新しいドメイン名が反映されるように、ノード名を更新する必要があります。
- ノード名が IP アドレスまたはホスト名の場合は、ドメインを参照していないので、何の変更も必要ありません。

ステップ 4 コマンドライン インターフェイス (CLI) を使用して、すべての該当するノードで DNS ドメインを更新します。CLI コマンドは、ノードのオペレーティングシステムで必要なドメイン変更を行い、各ノードの自動リブートを実行します。

ステップ 5 ドメイン名の更新後、クラスタ内のすべてのノードの「A Cisco DB」サービスを再起動して、すべてのノードのオペレーティングシステムの設定ファイルで、変更されたノードに関連付けられた DNS ドメイン名の変更が確実に有効になるようにします。

(注) システムが正しく機能していることを確認します。レプリケーションの問題が発生した場合は、クラスタ内のすべてのノードを再起動してください。

ステップ 6 CLI を使用してデータベース レプリケーションを確認します。詳細については、システムヘルス チェックの実行およびデータベース レプリケーションのトラブルシューティングに関連したトピックを参照してください。クラスタにあるすべてのシステムファイルが互いに同期した後で、データベースのレプリケーションを確認する必要があります。

ステップ 7 ノードのセキュリティ証明書を再生成します。

- すべての IM and Presence Service のセキュリティ証明書で、件名 CN がノード FQDN に設定されます。したがって、新しいノードドメインを取り入れるために、DNS ドメインの変更後は、すべての証明書が自動的に再生成されます。
- 証明書によって以前に署名された証明書。

ステップ 8 クラスタ内の該当するすべてのノードで変更後タスクを実行し、クラスタが正常に動作することを確認します。

DNS レコードの更新

ノードの DNS ドメインを変更するため、そのノードに関連付けられているすべての既存の DNS レコードを更新する必要があります。この対象となるレコードは、次のタイプのレコードです。

- A レコード
- PTR レコード
- SRV レコード

クラスタにある複数のノードを変更する場合は、それらのノードごとに以下の手順を実行する必要があります。

IM and Presence データベース パブリッシャ ノードを変更する場合は、該当する IM and Presence Service サブスクリバ ノードで手順を繰り返す前に、IM and Presence データベース パブリッシャ ノードでこの手順が完了している必要があります。



- (注)
- これらの DNS レコードの更新は、ノードでの DNS ノードの変更そのものを実行したメンテナンス時間の中で実行する必要があります。
 - スケジュールされているメンテナンス時間の前に DNS レコードを更新すると、IM and Presence Service の機能に影響が及ぶ可能性があります。

始める前に

導入ですべての変更前のタスクと該当するシステムヘルス チェックを実行します。

手順

- ステップ 1** ノードの古い DNS 順方向 (A) レコードを、古いドメインから削除します。
- ステップ 2** 新しいドメインに、このノードの新しい DNS 順方向 (A) レコードを作成します。
- ステップ 3** このノードの DNS 逆方向 (PTR) レコードを更新し、ノードの更新された完全修飾ドメイン名 (FQDN) を指すようにします。
- ステップ 4** このノードを指している DNS SRV レコードをすべて更新します。
- ステップ 5** このノードを指している他の DNS レコードをすべて更新します。
- ステップ 6** 各ノードでコマンドラインインターフェイス (CLI) コマンドを実行して、クラスタにある他のすべてのノードに上記の DNS の変更がすべて伝播されていることを確認します。
- a) 新しい A レコードを検証するには、`utils network host new-fqdn` を入力します。ここで、`new-fqdn` はノードの更新 FQDN です。

例 :

```
admin: utils network host server1.new-domain.com Local Resolution:
server1.new-domain.com resolves locally to 10.53.50.219 External Resolution:
server1.new-domain.com has address 10.53.50.219
```

- b) 更新 PTR レコードを検証するには、`utils network host ip-addr` を入力します。ここで、`ip-addr` はノードの IP アドレスです。

```
admin: utils network host 10.53.50.219 Local Resolution: 10.53.50.219
resolves locally to server1.new-domain.com External Resolution:
server1.new-domain.com has address 10.53.50.219 219.50.53.10.in-addr.arpa
domain name pointer server1.new-domain.com.
```

(注) 手順のこの時点では、ノードの DNS ドメインを変更しない限り、IP アドレスのローカル解決は古い FQDN を指したままになっています。

- c) 更新された SRV レコードを検証するには、`utils network host srv-name srv` を入力します。ここで、`srv-name` は SRV レコードです。

例 :

`_xmpp-server` SRV レコード検索の例。

```
admin: utils network host _xmpp-server._tcp.galway-imp.com srv Local
Resolution: Nothing found External Resolution: _xmpp-server._tcp.sample.com
has SRV record 0 0 5269 server1.new-domain.com.
```

次のタスク

IM and Presence Service ノード名を更新します。

FQDN 値での ノード名の更新

Cisco Unified CM IM and Presence 管理 GUI の [プレゼンス トポロジ (Presence Topology)] ウィンドウのノード用に定義されたノード名が、ノードの完全修飾ドメイン名 (FQDN) に設定されている場合、古いドメイン名が参照されます。したがって、新しいドメイン名を参照するようにノード名を更新する必要があります。



- (注) この手順は、このノードのノード名の値が FQDN に設定されている場合にのみ実行する必要があります。ノード名がノードの IP アドレスまたはホスト名と一致している場合、この手順は不要です。

クラスタにある複数のノードを変更する場合は、それらのノードごとに以下の手順を順番に実行する必要があります。

IM and Presence データベース パブリッシャ ノードを変更する場合、IM and Presence Service サブスクリバノードで以下の手順を最初に完了してから、パブリッシャ ノードの手順を完了する必要があります。

始める前に

ノードの DNS レコードを更新します。

手順

ステップ 1 IM and Presence Service ノードのノード名を変更します。

- Cisco Unified Communications Manager Administration にサインインします。
- [システム (System)] > [サーバ (Server)] を選択します。
- ノードを検索して選択します。
- FQDN が新しいドメイン値を参照するように [完全修飾ドメイン名/IP アドレス (Fully Qualified Domain Name/IP Address)] フィールドを更新します。たとえば、[完全修飾ドメイン名/IP アドレス (Fully Qualified Domain Name/IP Address)] の値を `server1.old-domain.com` から `server1.new-domain.com` に更新します。
- [保存] を選択します。

ステップ 2 Cisco Unified CM IM and Presence Administration GUI の [プレゼンス トポロジ (Presence Topology)] ウィンドウで、このノードのアプリケーションサーバのエントリが、新しいノード名を反映して更新されていることを確認します。

- Cisco Unified Communications Manager Administration にサインインし、[システム (System)] > [アプリケーションサーバ (Application Server)] を選択します。
- [アプリケーションサーバの検索/一覧表示 (Find and List Application Servers)] ウィンドウで、必要に応じて、[検索 (Find)] をクリックします。
- アプリケーションサーバのリストに、更新したノード名に対してエントリが存在することを確認します。

- (注) このノードのエントリが存在しない場合、またはそのエントリがあっても、ノードの古いノード名を反映している場合は、以降の手順には進まないでください。

次のタスク

該当するすべてのノードで DNS ドメインを更新します。

DNS ドメインの更新

コマンドライン インターフェイス (CLI) を使用して、IM and Presence Service ノードの DNS ドメインを変更できます。

全社的な IM and Presence Service のドメインは、IM and Presence Service ノードのネットワーク レベルの DNS デフォルト ドメインに対応している必要はありません。導入環境で企業全体のドメインを変更するには、『*Deployment Guide for IM and Presence Service on Cisco Unified Communications Manager*』を参照してください。

クラスタ内で複数のノードを変更する場合、ノードごとに以下の手順を順番に実行する必要があります。

IM and Presence データベース パブリッシャ ノードを変更する場合、サブスクライバ ノードを変更する前に、まずデータベースパブリッシャ ノードでこの手順を実行する必要があります。

始める前に

IM and Presence Service ノード名を更新します。

手順

- ステップ 1** ノードで CLI にサインインし、`set network domain new-domain` と入力します。new-domain は設定される新しいドメインの値です。

例 :

```
admin: set network domain new-domain.com *** W A R N I N G *** Adding/deleting
or changing domain name on this server will break database replication. Once
you have completed domain modification on all systems that you intend to
modify, please reboot all the servers in the cluster. This will ensure that
replication keeps working correctly. After the service is rebooted, please
confirm that there are no issues reported on the Cisco Unified Reporting report
for Database Replication. The server will now be rebooted. Do you wish to
continue. Security Warning : This operation will regenerate all CUP Certificates
including any third party signed Certificates that have been uploaded. Continue
(y/n)?
```

- ステップ 2** ドメインの変更を確認してノードをリブートする場合は `y` と入力してリターン キーを押し、キャンセルする場合は `n` と入力します。

ヒント ノード名の変更が完了すると、すべての証明書がノードで再生成されます。これらの証明書の中に、サードパーティの認証局で署名したものがあある場合、この手順の後半で、それらの署名済み証明書を再度要求する必要があります。

ステップ 3 ノードが再起動したら、`show network eth0` と入力して、ドメイン名の変更が有効になっていることを確認します。

例：

次の例での新しいドメインは `new-domain.com` です。

```
admin: show network eth0 Ethernet 0 DHCP : disabled Status : up IP Address :
10.53.50.219 IP Mask : 255.255.255.000 Link Detected: yes Mode : Auto disabled,
Full, 1000 Mbits/s Duplicate IP : no DNS Primary : 10.53.51.234 Secondary :
Not Configured Options : timeout:5 attempts:2 Domain : new-domain.com Gateway
: 10.53.50.1 on Ethernet 0
```

ステップ 4 クラスタ内のすべての該当するノードに対して前の手順を繰り返して行います。

次のタスク

クラスタのすべてのノードをリブートします。

クラスタ ノードに関する考慮事項

コマンドライン インターフェイス (CLI) を使用して、クラスタ内のノードで「A Cisco DB」サービスを再起動できます。

ドメイン名を変更してノードを再起動したら、自動的に再起動したノードを含む、クラスタ内のすべてのノードの「A Cisco DB」サービスを再起動する必要があります。Unified CM Publisher から始めて、公開されたデータベースが表示されると、すべてのサブスクリバに適用されます。これによって、すべてのノードで、オペレーティングシステムのコンフィギュレーション ファイルを、新しいドメインの値に一致したものにすることができます。

システムが正しく機能していることを確認します。レプリケーションの問題が発生した場合は、クラスタ内のすべてのノードを再起動してください。

最初に IM and Presence データベース パブリッシャ ノードのリブート プロセスを開始します。データベース パブリッシャ ノードが再起動したら、次に残りの IM and Presence Service サブスクリバ ノードのリブートを任意の順序で実行します。

始める前に

ノードの DNS ドメイン名が変更されたことを確認します。

手順

ステップ 1 CLI を使用して IM and Presence データベース パブリッシャ ノードをリブートします。 `utils system restart` を入力します。

例 :

```
admin: utils system restart Do you really want to restart ? Enter (yes/no)?
```

ステップ 2 `yes` を入力して、再起動して **Return** キーを押します。

ステップ 3 IM and Presence データベース パブリッシャ ノードが再起動したことを示す次のメッセージが表示されるまで待ちます。

例 :

```
Broadcast message from root (Wed Oct 24 16:14:55 2012): The system is going down for reboot NOW! Waiting . Operation succeeded restart now.
```

ステップ 4 各 IM and Presence Service サブスクリバノードの CLI にサインインし、 `utils system restart` を入力して各サブスクリバノードをリブートします。

(注) サービスの停止を試行してから数分が経過すると、CLI から再起動するよう求められることがあります。その場合は `yes` を入力します。

次のタスク

データベースのレプリケーションを確認します。詳細については、システムヘルスチェックに関するトピックを参照してください。

セキュリティ証明書の再生成

ノードの完全修飾ドメイン名 (FQDN) は、すべての IM and Presence Service セキュリティ証明書で件名 CN として使用されます。したがって、ノードで DNS ドメインを更新すると、すべてのセキュリティ証明書が自動的に再生成されます。

いずれかの証明書にサードパーティの認証局が署名していた場合は、認証局が署名した証明書を新たに手動で生成する必要があります。

クラスタにある複数のノードを変更する場合は、ノードごとに以下の手順を実行する必要があります。



(注) ノードのデフォルトドメイン名を変更する前に、新しい証明書を要求することはできません。証明書署名要求 (CSR) の生成は、ノードでドメインを変更し、そのノードを再起動した後のみ可能です。

始める前に

データベース レプリケーションがすべてのノードで正常に確立されるように、データベース レプリケーションを確認します。

手順

- ステップ 1** 証明書にサードパーティの認証局による署名が必要な場合は、Cisco Unified Operating System Administration GUI にサインインし、関連する証明書ごとに必要な手順を実行します。
- ステップ 2** 署名付き証明書をアップロードしたら、IM and Presence Service ノードでサービスの再起動が必要になることがあります。

再起動が必要になるサービスは次のとおりです。

- Tomcat 証明書：次のコマンドライン インターフェイス (CLI) のコマンドを実行して、Tomcat サービスを再起動します。

```
utils service restart Cisco Tomcat
```
- CUP-xmpp 証明書：Cisco Unified Serviceability GUI から Cisco XCP Router サービスを再起動します。
- Cup-xmpp-s2s 証明書：Cisco Unified Serviceability GUI から Cisco XCP Router サービスを再起動します。

- (注)
- これらのアクションによって、影響を受けるサービスが再起動します。したがって、署名済み証明書を入手するまでに要する時間に応じて、再起動をより遅いメンテナンス時間でスケジュールする必要が生じる場合があります。サービスを再起動するまでの間は、暫定的に自己署名の証明書が関連のインターフェイスに引き続き提示されます。
 - 上記のリストで指定されていない証明書では、サービスの再起動は不要です。

次のタスク

クラスタ内のすべての該当するノードで、変更後のタスク リストを実行します。

ノード名の変更

IM and Presence Service ノードまたはノード グループに関連付けられたノード名を変更できます。更新は、[Cisco Unified Communications Manager Administration] の [サーバの設定 (Server Configuration)] ウィンドウに表示されます。

次のノード名変更シナリオでこれらの手順を使用します。

- IP アドレスからホスト名へ

- IP アドレスから完全修飾ドメイン名 (FQDN) へ
- ホスト名から IP アドレスへ
- ホスト名から FQDN へ
- FQDN からホスト名へ
- FQDN から IP アドレスへ

ノード名の推奨事項について詳しくは、『*Deployment Guide for IM and Presence Service on Cisco Unified Communications Manager*』を参照してください。



注意 ネットワーク レベルの変更が必要とされていない IM and Presence Service ノードでのみノード名を変更するには、以下の手順を使用します。その場合は、ネットワーク IP アドレス、ホスト名、またはドメイン名の変更に固有の手順を実行します。このノード名の変更手順は、スケジュールしたメンテナンス時間内に実行する必要があります。IM and Presence Service クラスタでいずれかのノードのノード名を変更すると、ノードが再起動し、Presence サービスやその他のシステム機能に割り込みます。

IM and Presence Service ノード名の変更作業リスト

次の表に、IM and Presence Service ノードまたはノード グループに関連付けられたノード名を変更するためのステップごとの手順を示します。この手順の詳しい説明では、変更を実行するステップの正確な順序を指定しています。

複数のクラスタにわたってこの手順を実行する場合は、順番に一度に1つのクラスタでノード名を変更する手順を完了します。

表 84: IM and Presence Service ノード名の変更の作業リスト

項目	タスク
1	クラスタ内のすべての該当するノードで変更前の作業を完了します。変更前の作業の一部は IM and Presence データベース パブリッシャ ノードだけに適用し、サブスクライバ ノードを変更する場合はスキップすることができます。
2	Cisco Unified Communications Manager Administration を使用して、IM and Presence Service ノード名を更新します。
3	ノード名の更新を確認し、ノード名の変更が IM and Presence Service と確実に同期されるようにします。
4	ノード名の更新の完了後に、コマンドライン インターフェイス (CLI) を使用してデータベース レプリケーションを確認します。新しいノード名がクラスタで複製されていることと、データベース レプリケーションがすべてのノードで動作することを確認します。

項目	タスク
5	更新されたノードで変更後の作業リストを完了し、ノードが正常に動作することを確認します。

ノード名の更新

クラスタにある複数のノードを変更する場合は、それらのノードごとに以下の手順を順番に実行する必要があります。

IM and Presence データベース パブリッシャ ノードを変更する場合、IM and Presence Service サブスクライバ ノードで以下の手順を最初に完了してから、パブリッシャ ノードの手順を完了する必要があります。



(注) IM and Presence ノードの場合は、完全修飾ドメイン名を使用することをお勧めします。ただし、IP アドレスとホスト名もサポートされています。

始める前に

導入環境で、すべての変更前タスクと該当するシステムヘルスチェックを実行します。

手順

ステップ 1 [Cisco Unified CM 管理] ページにサインインします。

ステップ 2 [システム (System)] > [サーバ (Server)] を選択します。

ステップ 3 変更するノードを選択します。

ステップ 4 新しいノード名を使用して、[ホスト名/IP アドレス (Host name/IP Address)] フィールドを更新します。

(注) 新しく生成された SP メタデータを IDP サーバにアップロードしていることを確認します。

ステップ 5 クラスタ内の複数のノードを変更する場合は、ノードごとにこの手順を繰り返して行います。

(注) IM and Presence Service ノード名を更新する際に、サードパーティのコンプライアンスも設定されている場合は、ノード名に基づく新しいレルムを使用するようにコンプライアンス サーバを更新する必要があります。この設定の更新は、サードパーティのコンプライアンスサーバで行われます。新しいレルムは、[Cisco Unified CM IM and Presence Administration] > [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)] ウィンドウに表示されます。

始める前に

IM and Presence Service ノード名を更新します。

手順

- ステップ 1 Cisco Unified CM IM and Presence Administration GUI にサインインします。
- ステップ 2 [システム (System)] [プレゼンス トポロジ (Presence Topology)] を選択します。
- ステップ 3 新しいノード名が既存の [プレゼンス トポロジ (Presence Topology)] ペインに表示されていることを確認します。

次のタスク

データベースのレプリケーションを確認します。

Cisco Unified Communications Manager のドメイン名の更新

CLI (コマンドライン インターフェイス) を使用して、Cisco Unified Communications Manager のドメイン名を変更できます。CLI を使用して、該当するすべてのノードで DNS ドメイン名を更新します。CLI コマンドは、ノードに必要なドメイン名変更を行い、各ノードの自動リブートを実行します。

Unified CM クラスターのセキュリティモードが非セキュアであり、ドメインを更新または変更している場合、ドメインの変更の一環として、すべての証明書が再生成されます。電話で ITL が更新されていることを確認するには、ドメイン名を更新する前に必要な次の手順を実行します。

1. 更新された ITL を処理できるようにすべての電話機が登録され、オンラインであることを確認します。この手順を実行するときに電話機がオンラインでない場合は、ITL を手動で削除する必要があります。
2. [Prepare Cluster for Rollback to pre-8.0] エンタープライズ パラメータを [True] に設定します。すべての電話機は自動的にリセットされ、空の信頼検証サービス (TVS) と TFTP 証明書セクションを含む ITL ファイルがダウンロードされます。
3. 電話機で、[設定 (Settings)] > [セキュリティ (Security)] > [信頼リスト (Trust List)] > [ITL ファイル (ITL File)] の順に選択し、ITL ファイルの TVS および TFTP 証明書セクションが空であることを確認します。
4. サーバのドメインを変更し、クラスターへの登録がロールバックされるように電話機を設定します。

5. すべての電話機がクラスタに正常に登録されたら、エンタープライズ パラメータ **Prepare Cluster for Rollback to pre-8.0** を **False** に設定します。

始める前に

- ドメイン名を変更する前に、必ず DNS を有効にしてください。
- サーバテーブルに既存のホスト名エントリがある場合は、最初にドメイン名のホスト名エントリを変更します。
- すべての変更前タスクと該当するシステムヘルスチェックを実行します。詳細については、「関連項目」を参照してください。

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 **Run set network domain < new_domain_name >**を入力します。
コマンドは、システムの再起動を求めるプロンプトを表示します。
 - ステップ 3 [はい (Yes)] をクリックしてシステムをリブートします。
システムの再起動後に、新しいドメイン名が更新されます。
 - ステップ 4 **Show network eth0** コマンドを入力して、再起動後に新しいドメイン名が更新されているかどうかを確認します。
 - ステップ 5 すべてのクラスタ ノードに対してこの手順を繰り返します。
-

次のタスク

導入の変更が正しく実行されていることを確認するすべての該当する変更後の作業を実行します。詳細については、「関連項目」を参照してください。



第 32 章

変更後のタスクと検証

- [Cisco Unified Communications Manager ノードの変更後タスク \(465 ページ\)](#)
- [Cisco Unified Communications Manager ノードのセキュリティを有効にしたクラスタ タスク \(469 ページ\)](#)
- [IM and Presence Service ノードの変更後タスク \(470 ページ\)](#)

Cisco Unified Communications Manager ノードの変更後タスク

変更後タスクすべてを実行し、導入環境に変更が適切に実装されていることを確認してください。



注意 これらのタスクを実行しても期待する結果が得られない場合は、問題が解決されるまで続行しないでください。

手順

- ステップ 1** Cisco Unified Communications Manager サーバ内で DNS が設定されている場合、正引きおよび逆引き参照ゾーンが設定され、DNS が到達可能で作動していることを確認します。
- ステップ 2** アクティブな ServerDown 警告が出ていないことを確認し、クラスタ内のすべてのサーバが稼働していて利用可能であることを確かめます。最初のノードで、Cisco Unified Real-Time Monitoring Tool (RTMT) またはコマンドラインインターフェイス (CLI) のいずれかを使用します。
- a) Unified RTMT を使用して確認するには、Alert Central にアクセスし、ServerDown 警告が発生していないか調べます。
 - b) 最初のノードで CLI を使用して確認するには、次の CLI コマンドを入力してアプリケーションのイベントログを調べます。

```
file search activelog syslog/CiscoSyslog ServerDown
```

ステップ 3 クラスタにあるすべてのノードでデータベースレプリケーションのステータスを調べ、すべてのサーバがデータベースの変更内容を正常に複製していることを確認します。

IM and Presence Service の場合、導入環境に複数のノードがあるときにはデータベースパブリッシャ ノードでデータベースレプリケーションのステータスを調べます。

Unified RTMT または CLI を使用します。すべてのノードで **2** のステータスが表示される必要があります。

- a) RTMT を使用して確認するには、Database Summary にアクセスしてレプリケーションのステータスを調べます。
- b) CLI を使用して確認するには、`utils dbreplication runtimestate` を入力します。
出力例については、データベースレプリケーションの出力例に関するトピックを参照してください。詳細な手順およびトラブルシューティングについては、データベースレプリケーションおよびデータベースレプリケーションのトラブルシューティングについてのトピックを参照してください。

ステップ 4 次の例に示されているように CLI コマンド `utils diagnose` を入力し、ネットワーク接続と DNS サーバの設定を確認してください。

例：

```
admin: utils diagnose module validate_network Log file:
/var/log/active/platform/log/diag1.log Starting diagnostic test(s)
===== test - validate_network : Passed Diagnostics
Completed admin:
```

変更前のシステムヘルスチェックを行っている場合には、これで完了です。そうでない場合には、変更後の確認手順を続行してください。

ステップ 5 Cisco Unified Communications Manager サーバリストに新しいホスト名または IP アドレスがあることを確認します。[Cisco Unified CM の管理 (Cisco Unified Communications Manager Administration)] で、[システム (System)] > [サーバ (Server)] を選択します。

(注) このステップは、変更後タスクの一部としてのみ実行します。

ステップ 6 IP アドレス、ホスト名、またはその両方に加えられた変更がネットワーク上で確実に実装されていることを確認します。クラスタ内の各ノードで CLI コマンド `show network cluster` を入力します。

(注) このステップは、変更後タスクの一部としてのみ実行します。

出力には、ノードの新しい IP アドレスまたはホスト名が含まれている必要があります。

例：

```
admin:show network cluster 10.63.70.125 hippo2.burren.pst hippo2 Subscriber
cups DBPub authenticated 10.63.70.48 aligator.burren.pst aligator Publisher
callmanager DBPub authenticated using TCP since Wed May 29 17:44:48 2013
```

ステップ 7 ホスト名に対する変更内容がネットワークで完全に実装されていることを確認します。クラスタ内の各ノードで CLI コマンド `utils network host <new_hostname>` を入力します。

(注) このステップは、変更後タスクの一部としてのみ実行します。

出力で、新しいホスト名が対象 IP アドレスに外部解決されていることを確認してください。

例 :

```
admin:utils network host hippo2 Local Resolution: hippo2.burren.pst resolves locally to 10.63.70.125 External Resolution: hippo2.burren.pst has address 10.63.70.125
```

タスク。

ステップ 8 セキュリティが有効になっているクラスタ (クラスタセキュリティモード 1-混合) の場合、CTL ファイルを更新し、クラスタ内のすべてのノードを再起動してから、システムヘルスチェックと他の変更後タスクを実行します。

詳細については、[マルチサーバクラスタ電話機の証明書と ITL の再生成 \(470 ページ\)](#) を参照してください。

ステップ 9 証明書信頼リスト (CTL) ファイルと USB eToken を使用してクラスタセキュリティを有効にした場合、リリース 8.0 以降のノードの IP アドレスまたはホスト名を変更した際は、Initial Trust List (ITL; 初期信頼リスト) ファイルと ITL の証明書を再生成する必要があります。クラスタセキュリティの有効化に証明書信頼リスト (CTL) ファイルと USB eToken を使用していない場合は、このステップをスキップしてください。

ステップ 10 手動で DRS バックアップを実行し、すべてのノードとアクティブなすべてのサービスが正しくバックアップされていることを確認します。

詳細については、『*Administration Guide for Cisco Unified Communications Manager*』を参照してください。

(注) ノードの IP アドレスを変更した後は手動で DRS バックアップを実行する必要があります。これは、DRS ファイルでノードを復元するには、DRS ファイルとノードで IP アドレスとホスト名が一致している必要があるからです。変更後の DRS ファイルには、新しい IP アドレスや新しいホスト名が記録されています。

ステップ 11 関連する IP フォンの URL パラメータをすべて更新します。

ステップ 12 [Cisco Unified Communications Manager Administration] を使用して、関連するすべての IP フォンサービスを更新します。[システム(System)] > [エンタープライズパラメータ(Enterprise Parameters)] を選択します。

ステップ 13 Unified RTMT カスタム警告と保存済みプロファイルを更新します。

- パフォーマンスカウンタから得られた Unified RTMT カスタム警告には、サーバの IP アドレスがハードコードで記録されています。これらのカスタム警告を削除し、再設定する必要があります。

- パフォーマンス カウンタを備えた Unified RTMT 保存済みプロファイルには、サーバの IP アドレスがハードコードで記録されています。これらのカウンタをいったん削除してから追加し直した後、プロファイルを保存して新しい IP アドレスで更新する必要があります。

ステップ 14 Cisco Unified Communications Manager で動作する統合 DHCP サーバを使用している場合は、DHCP サーバを更新します。

ステップ 15 その他の関連する Cisco Unified Communications コンポーネントに対して、必要な設定変更を検査して実行します。

検査対象のコンポーネントの一部を次に示します。

- Cisco Unity
- Cisco Unity Connection
- CiscoUnity Express
- SIP/H.323 トランク
- IOS Gatekeeper
- Cisco Unified MeetingPlace
- Cisco Unified MeetingPlace Express
- Cisco Unified Contact Center Enterprise
- Cisco Unified Contact Center Express
- IP 電話向け DHCP Scopes
- CDR エクスポート用の Cisco Unified Communications Manager のトレース収集、または DRS バックアップの保存先として使用する SFTP サーバ
- Cisco Unified Communications Manager に登録されている IOS ハードウェア リソース（会議ブリッジ、メディアターミネーションポイント、トランスコーダ、RSVP エージェント）
- Cisco Unified Communications Manager に登録または統合した IPVC ビデオ MCU
- Cisco Emergency Responder
- Cisco Unified Application Environment
- Cisco Unified Presence
- Cisco Unified Personal Communicator
- 関連するルータおよびゲートウェイ

(注) 必要に応じて設定を変更する方法については、ご使用の製品のマニュアルを参照してください。

Cisco Unified Communications Manager ノードのセキュリティを有効にしたクラスタ タスク

初期信頼リストおよび証明書の再生成

Cisco Unified Communications Manager リリース 8.0 リリース以降のクラスタでサーバの IP アドレスまたはホスト名を変更すると、ITL の初期信頼リスト (ITL) ファイルと証明書が再生成されます。再生されたファイルは、電話機に保存されたファイルと一致しません。



- (注) 証明書信頼リスト (CTL) ファイルと USB eToken を使用してクラスタ セキュリティを有効にする場合は、eToken によって信頼が保持され、eToken は変更されないため、次の手順を実行する必要はありません。

クラスタ セキュリティが有効になっていない場合は、シングルサーバクラスタまたはマルチサーバクラスタでこの手順を実行して電話機をリセットします。

シングルサーバクラスタ電話機の証明書と ITL の再生成

Cisco Unified Communications Manager リリース 8.0 以降のシングルサーバクラスタでサーバの IP アドレスまたはホスト名を変更する際に、ITL ファイルを使用する場合、以下の手順を実行して電話機をリセットします。

サーバの IP アドレスまたはホスト名を変更する前に、ロールバックを有効にします。

手順

- ステップ 1** 更新された ITL を処理できるようにすべての電話機が登録され、オンラインであることを確認します。この手順を実行するときに電話機がオンラインでない場合は、ITL を手動で削除する必要があります。
- ステップ 2** Prepare Cluster for Rollback to pre-8.0 エンタープライズパラメータを True に設定します。すべての電話機は自動的にリセットされ、空の信頼検証サービス (TVS) と TFTP 証明書セクションを含む ITL ファイルがダウンロードされます。
- ステップ 3** 電話機で、[設定 (Settings)] > [セキュリティ (Security)] > [信頼リスト (Trust List)] > [ITL ファイル (ITL File)] の順に選択し、ITL ファイルの TVS および TFTP 証明書セクションが空であることを確認します。
- ステップ 4** サーバの IP アドレスまたはホスト名を変更し、クラスタへの登録がロールバックされるように電話機を設定します。

- ステップ 5** すべての電話機がクラスタに正常に登録されたら、エンタープライズパラメータ `PrepareCluster for Rollback to pre-8.0` を **False** に設定します。

次のタスク

CTL ファイルまたはトークンを使用する場合は、サーバの IP アドレスまたはホスト名を変更した後、または DNS ドメイン名を変更した後に、CTL クライアントを再実行します。

マルチサーバクラスタ電話機の証明書と ITL の再生成

マルチサーバクラスタでは、電話機が、再生成された ITL ファイルおよび証明書を確認するためのプライマリおよびセカンダリ TVS サーバを持つ必要があります。電話機がプライマリ TVS サーバに（最近の設定変更により）接続できない場合は、セカンダリサーバにフォールバックされます。TVS サーバは、電話機に割り当てられた CM グループによって識別されます。

マルチサーバクラスタでは、一度に 1 つのサーバだけで IP アドレスまたはホスト名を変更するようにしてください。CTL ファイルまたはトークンを使用する場合は、サーバの IP アドレスまたはホスト名を変更した後、または DNS ドメイン名を変更した後に、CTL クライアントまたは CLI コマンド `set utils ctl` を再実行します。

IM and Presence Service ノードの変更後タスク

変更後タスクすべてを実行し、導入環境に変更が適切に実装されていることを確認してください。



注意 これらのタスクを実行しても期待する結果が得られない場合は、問題が解決されるまで続行しないでください。

手順

- ステップ 1** ホスト名または IP アドレスに対する変更内容が、Cisco Unified Communications Manager サーバ上で更新されていることを確認します。
- ステップ 2** 変更したノードのネットワーク接続と DNS サーバの設定を確認してください。

(注) 異なるサブネットに IP アドレスを変更した場合は、ネットワークアダプタが正しい VLAN に接続されていることを確認します。また、IP アドレスの変更後に IM and Presence Service ノードが別のサブネットに属している場合、Cisco XCP Router サービスパラメータの [ルーティング通信タイプ (Routing Communication Type)] フィールドが [ルータ間 (Router to Router)] に設定されていることを確認してください。その他の場合には、[ルーティング通信タイプ (Routing Communication Type)] フィールドは [マルチキャスト DNS (Multicast DNS)] に設定する必要があります。

- ステップ 3** IP アドレス、ホスト名、またはその両方への変更がネットワークで完全に実装されていることを確認してください。
- ステップ 4** ホスト名を変更した場合は、ネットワークでホスト名の変更が確実に実装されていることを確認します。
- ステップ 5** データベース レプリケーションが正常に確立されたことを確認します。すべてのノードのステータスが 2 で、[接続済み (Connected)] になっている必要があります。レプリケーションがセットアップされていない場合、データベース レプリケーションの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。
- ステップ 6** SAML シングルサインオン (SSO) を無効にした場合、ここで有効にできます。SAML SSO の詳細については、『*Deployment Guide for IM and Presence Service on Cisco Unified Communications Manager*』を参照してください。
- ステップ 7** ホスト名を変更した場合、cup、cup-xmpp、および Tomcat の証明書に新しいホスト名が含まれていることを確認する必要があります。
- Cisco Unified OS Administration GUI から、[セキュリティ (Security)] > [証明書の管理 (Certificate Management)] を選択します。
 - 信頼証明書の名前に新しいホスト名が含まれていることを確認します。
 - 証明書に新しいホスト名が含まれない場合、証明書を再生成します。
- 詳細については、『*Administration Guide for Cisco Unified Communications Manager*』を参照してください。
- ステップ 8** ノードの IP アドレスを変更したら、Cisco Unified Real-Time Monitoring Tool (RTMT) のカスタムアラートと保存済みプロファイルを更新してください。
- パフォーマンスカウンタから得られた RTMT カスタム警告には、サーバのアドレスがハードコードで記録されています。これらのカスタム警告を削除し、再設定する必要があります。
 - パフォーマンスカウンタを備えた RTMT 保存済みプロファイルには、サーバのアドレスがハードコードで記録されています。これらのカウンタをいったん削除してから追加し直した後、プロファイルを保存して新しいアドレスで更新する必要があります。
- ステップ 9** その他の関連する Cisco Unified Communications のコンポーネント (たとえば Cisco Unified Communications Manager の SIP トランクなど) に必要な設定変更を確認し、変更を行ってください。
- ステップ 10** Cisco Unified Serviceability を使用して CUP サービス グループの下にリストされるすべてのネットワーク サービスを開始するには、[ツール (Tools)] > [コントロールセンターのネットワーク サービス (Control Center - Network Services)] を選択します。
- ヒント** IP アドレス、ホスト名、または IP アドレスとホスト名の両方を変更する場合、この手順を実行する必要はありません。これらの名前を変更した場合、ネットワーク サービスは自動的に開始します。しかし、変更後に一部のサービスが自動的に開始されない場合には、この手順を実行して、すべてのネットワーク サービスが確実に開始されるようにしてください。

次の順序で CUP サービスのネットワーク サービスを開始する必要があります。

1. Cisco IM and Presence Data Monitor
2. Cisco Server Recovery Manager
3. Cisco Route Datastore
4. Cisco Login Datastore
5. Cisco SIP Registration Datastore
6. Cisco Presence Datastore
7. Cisco XCP Config Manager
8. Cisco XCP Router
9. Cisco OAM Agent
10. Cisco Client Profile Agent
11. Cisco Intercluster Sync Agent
12. Cisco Config Agent

ステップ 11 Cisco Unified Serviceability を使用してすべての機能サービスを開始するには、[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)] を選択します。機能サービスを開始する順序は重要ではありません。

ヒント IP アドレス、ホスト名、または IP アドレスとホスト名の両方を変更する場合は、この手順を実行する必要はありません。これらの名前を変更した場合、機能サービスは自動的に開始します。しかし、変更後に一部のサービスが自動的に開始されない場合には、この手順を実行して、すべての機能サービスが確実に開始されるようにしてください。

ステップ 12 ハイアベイラビリティを再度有効にする前に Cisco Jabber セッションが再作成されたことを確認します。そうしないと、セッションが作成された Jabber クライアントが接続できなくなります。

すべてのクラスタノードで `show perf query counter "Cisco Presence Engine" ActiveJsmSessions` CLI コマンドを実行します。アクティブセッションの数は、ハイアベイラビリティを無効にした際に記録したユーザ数と一致するはずです。セッションが開始されるまでに30分以上かかる場合は、システムの問題が大きくなる可能性があります。

ステップ 13 変更前のセットアップ中にハイアベイラビリティ (HA) を無効にした場合、すべてのプレゼンス冗長グループの HA を有効にします。

ステップ 14 IM and Presence サービスが変更後に正しく機能していることを確認します。

- a) Cisco Unified Serviceability GUI から、[システム (System)] > [プレゼンストポロジ (Presence Topology)] を選択します。
 - HA が有効の場合は、すべての HA ノードが [正常 (Normal)] 状態であることを確認します。
 - すべてのサービスが開始されていることを確認します。
- b) Cisco Unified CM IM and Presence Administration GUI からシステムトラブルシュータを実行し、失敗したテストがないことを確認します。[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 15 ノードの IP アドレスまたはホスト名を変更した後は、手動でディザスタ リカバリ システム バックアップを実行する必要があります。これは、DRS ファイルでノードを復元するには、DRS ファイルとノードで IP アドレスとホスト名が一致している必要があるからです。変更後の DRS ファイルには、新しい IP アドレスや新しいホスト名が記録されています。

詳細については、『*Administration Guide for Cisco Unified Communications Manager*』を参照してください。



第 33 章

アドレス変更に関する問題のトラブルシューティング

- クラスタ認証のトラブルシューティング (475 ページ)
- データベース レプリケーションのトラブルシューティング (476 ページ)
- ネットワークをトラブルシューティング (481 ページ)
- ネットワーク タイム プロトコル (NTP) のトラブルシューティング (482 ページ)

クラスタ認証のトラブルシューティング

コマンドラインインターフェイス (CLI) を使用して、サブスライバノードのクラスタ認証問題をトラブルシューティングできます。

手順

ステップ 1 ネットワーク設定を確認するために、`show network eth0 [detail]` を入力します。

ステップ 2 `show network cluster` を入力して、ネットワークのクラスタ情報を確認します。

- 誤ったパブリッシャ情報が出力に表示されている場合は、サブスライバノードで `set network cluster publisher [ホスト名/IP アドレス]` CLI コマンドを入力して情報を修正します。
- パブリッシャノードで、誤ったサブスライバ情報が `show network cluster` CLI コマンドに表示される場合、Cisco Unified CM の管理にログインして、[システム (System)] > [サーバ (Server)] を選択し、出力を検査します。
- サブスライバノードで、`show network cluster` の出力に誤ったパブリッシャ情報が表示されている場合は、`set network cluster publisher [hostname | IP_address]` CLI コマンドを使用して、パブリッシャのホスト名または IP アドレスを変更します。

データベース レプリケーションのトラブルシューティング

コマンドラインインターフェイス (CLI) を使用して、クラスタのノードにおけるデータベース レプリケーションをトラブルシューティングできます。

- データベース レプリケーションがクラスタ内で適切な状態にあることを確認します。
- ノードのデータベース レプリケーションを修復して再確立します。
- データベース レプリケーションをリセットします。

これらのコマンドまたは CLI の使用方法の詳細については、『*Command Line Interface Guide for Cisco Unified Communications Solutions*』を参照してください。

データベースのレプリケーションの確認

コマンドラインインターフェイス (CLI) を使用して、クラスタ内のすべてのノードでデータベース レプリケーションのステータスを確認します。Replication Setup (RTMT) & Details に 2 の値が表示されていることを確認します。この値が 2 以外になっている場合は、データベースのレプリケーションに何らかの問題があるので、ノードのレプリケーションをリセットする必要があります。出力例については、データベース レプリケーションの例に関連したトピックを参照してください。

手順

ステップ 1 クラスタ内のすべてのノードでデータベース レプリケーションを検査するには、最初のノードで `utils dbreplication runtimestate` と入力します。

IM and Presence Service では、導入に複数のノードがある場合、データベース パブリッシャ ノードでこのコマンドを入力します。

ヒント レプリケーションがクラスタ内のノードに設定されていない場合は、CLI を使用してノードのデータベース レプリケーションをリセットできます。詳細については、CLI を使用したデータベース レプリケーションのリセットに関するトピックを参照してください。

例 :

```
admin: utils dbreplication runtimestate DDB and Replication Services: ALL
RUNNING DB CLI Status: No other dbreplication CLI is running... Cluster
Replication State: BROADCAST SYNC Completed on 1 servers at: 2013-09-26-15-18
Last Sync Result: SYNC COMPLETED 257 tables syncmonitorout of 257 Sync Errors:
NO ERRORS DB Version: ccm9_0_1_10000_9000 Number of レプリケート tables: 257
Repltimeout set to: 300sPUB (2 サーバ) からのクラスタ詳細ビュー: レプリケーション複製
を PING します。DBver& REPL. REPLICATION SETUP SERVER-NAME IP ADDRESS (ミリ秒)
RPC? STATUS QUEUE TABLES LOOP? (RTMT) & details -----
----- server1 100.10.10.17
```

```
0.052 Yes Connected 0 match Yes (2) PUB Setup Completed server2 100.10.10.14
0.166 Yes Connected 0 match Yes (2) Setup Completed
```

ステップ 2 出力を確認します。

出力では、各ノードの REPLICATION STATUS が **Connected**、および REPLICATION SETUP 値が **(2) Setup Complete** として表示される必要があります。これはクラスタ内のレプリケーション ネットワークが正しく動作していることを意味します。出力結果が異なる場合は、データベース レプリケーションのトラブルシューティングと修復に進みます。

データベース レプリケーションの CLI 出力例

次のリストは、クラスタの最初のノードで `utils dbreplication runtimestate` コマンドライン インターフェイス (CLI) コマンドを実行した場合に `Replicate_State` として可能な値を示しています。

IM and Presence Service では、導入に複数のノードがある場合、データベース パブリッシャ ノードでこのコマンドを入力します。

- 0: レプリケーションが開始しない。これは、サブスクリバが存在していないか、またはサブスクリバをインストールした後に Database Layer Monitor サービスが実行されていないことが原因です。
- 1: レプリケーションは作成されていますが、そのカウントが正しくありません。
- 2: レプリケーションは良好である。
- 3: クラスタ内のレプリケーションは不良である。
- 4: レプリケーションのセットアップに成功しませんでした。



(注) [レプリケーションのセットアップ (RTMT) と詳細 (Replication Setup (RTMT) & Details)] に値 2 が示されていることが重要です。この値が 2 以外になっている場合は、データベースのレプリケーションに何らかの問題があるので、レプリケーションをリセットする必要があります。データベース レプリケーションの問題の解決方法については、データベース レプリケーションの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。

Cisco Unified Communications Manager ノードの CLI 出力例

この例では、Replication Setup (RTMT) & Details に 2 の値が表示されています。レプリケーションは良好です。

```
admin:ユーティリティ dbreplication runtimestate Server Time: Mon 6 月 1 12:00:00 EDT
2013 クラスタレプリケーションの状態: ブロードキャスト同期が完了しました。 2013-06-01-12-00
Last SYNC RESULT: SYNC Completed on 672 tables out Of 672 SYNC STATUS: NO
```

```

ERRORS Use CLI to see detail: ' file view activelog
cm/trace/cdr/2013_06_01_12_00_00_dbl_repl_output Broadcast. LOG ' DB Version:
  Ccm10_0_1_10000_1 repltimeout set to: 300s PROCESS option set to: 1 Cluster
Detailed view from uc10-pub (2 servers): PING ReplicationREPLICATION SETUP
SERVER-NAME IP ADDRESS (ミリ秒) RPC? Group ID (RTMT) & の詳細
-----uc10-pub 192.0.2.95
  0.040 Yes (g_2) (2) Setup Completed uc10-sub1 192.0.2.96 0.282 Yes (g_3) (2)
  Setup completed

```

IM and Presence Service ノードの CLI 出力例

この例では、Replication Setup (RTMT) & Details に 2 の値が表示されています。レプリケーションは良好です。

```

admin: のコマンドの実行時間: Mon 6 月 1 12:00:00 EDT 2013 DB およびレプリケーションサー
ビス: すべての RUNNING Cluster Replication State: replication status コマンドが開
始されました: 2012-02-26-09-40 Replication STATUS コマンド COMPLETED 269 tables
checked out Of 269 No Errors or ミスマッチ found. Use 'file view activelog
cm/trace/dbl/sdi/ReplicationStatus.2012_02_26_09_40_34.out' to see the details
DB Version: ccm8_6_3_10000_23 Number of replicated tables: 269 Cluster Detailed
View from PUB (2 Servers): PING REPLICATION REPL. DBver& REPL. REPLICATION
SETUP SERVER-NAME IP ADDRESS (ミリ秒) RPC? STATUS QUEUE TABLES LOOP? (RTMT) &
の詳細
-----gwydla020218
  10.53.46.130 0.038 Yes Connected 0 match Yes (2) PUB Setup Completed
gwydla020220 10.53.46.133 0.248 Yes Connected 128 match Yes (2)セットアップが完了
しました

```

データベース レプリケーションの修復

コマンドラインインターフェイス (CLI) を使用して、データベース レプリケーションを修復します。

手順

- ステップ 1** 最初のノードで `utils dbreplication repair all` と入力し、データベース レプリケーションの修復を試みます。

IM and Presence Service では、導入に複数のノードがある場合、データベース パブリッシャ ノードからデータベース レプリケーションのステータスを修復します。

データベースのサイズによっては、データベース レプリケーションの修復に数分を要することがあります。次の手順に進み、データベース レプリケーションの修復の進行状況を監視します。

例:

```
admin: ユーティリティの [replication repair all-----すべてのユーティ
リティの dbreplication repair-----レプリケーション修復がバックグラウン
ドで実行されるようになりました。 Use command 'utils dbreplication runtimestate' to
check its progress Output will be in file
cm/trace/dbl/sdi/ReplicationRepair.2013_05_11_12_33_57.out Please use "file
view activelog cm/trace/dbl/sdi/ReplicationRepair.2013_05_11_12_33_57.out "
command to see the output
```

ステップ 2 最初のノードで `utils dbreplication runtimestate` を入力して、レプリケーション修復の進行状況を確認します。

IM and Presence Service では、導入に複数のノードがある場合、データベースパブリッシャノードでこのコマンドを入力します。

レプリケーション出力例の太字にされたテキストは、レプリケーション修復の最終ステータスを示しています。

例：

```
管理者: ユーティリティ dbreplication runtimestate DB および Replication Services:
すべての実行中のクラスタレプリケーション状態: Replication repair コマンドが開始されまし
た: 2013-05-11-12-33 Replication repair コマンドが完了しました。269テーブルが269から
処理されました。エラーまたは不一致は見つかりませんでした。 Use 'file view activelog
cm/trace/dbl/sdi/ReplicationRepair.2013_05_11_12_33_57.out' to see the details
DB Version: ccm8_6_4_98000_192 Number of replicated tables: 269 Cluster Detailed
View from PUB (2 Servers): PING REPLICATION REPL. DBver& REPL. REPLICATION
SETUP SERVER-NAME IP ADDRESS (ミリ秒) RPC? STATUS QUEUE TABLES LOOP? (RTMT) &
details -----
----- server1 100.10.10.17 0.052 Yes Connected 0 match Yes (2) PUB
Setup Completed server2 100.10.10.14 0.166 Yes Connected 0 match Yes (2) Setup
Completed
```

- a) レプリケーションの修復がエラーや不一致なしで最後まで実行された場合、ノード名の変更を確認する手順をもう一度実行し、新しいノード名が正常に複製されたことを検証します。
- b) エラーまたは不一致が見つかった場合は、ノード間の一時的な不一致が存在する可能性があります。データベースレプリケーションを修復する手順をもう一度実行します。

(注) レプリケーションの修復を数回試行した後も、不一致またはエラーがレポートされる場合は、シスコのサポート担当者に連絡して問題を解決してください。

ステップ 3 最初のノードで `utils dbreplication reset all` と入力し、データベースレプリケーションの再確立を試みます。

IM and Presence Service では、導入に複数のノードがある場合、データベースパブリッシャノードでこのコマンドを入力します。

データベースのサイズによっては、データベースレプリケーションが完全に再確立するのに数分を要することがあります。次の手順に進み、データベースレプリケーションの再確立の進行状況を監視します。

例：

```
admin: shelldbreplication reset
```

すべてこのコマンドは、レプリケーションのリセットを開始しようとしても、1-2 分後に戻ります。複製のバックグラウンド修復は、その後1時間後に続行されます。RTMT のレプリケーションの状態を確認してください。0 ~ 2 の位置にする必要があります。すべてのサブで RTMT の複製状態が2に設定されている場合、レプリケーションは完了します。サブレプリケーションの状態が4または1になると、レプリケーションのセットアップでエラーが発生します。すべてのサブの RTMT カウンタをモニタして、レプリケーションが完了したことを確認します。エラーの詳細が見つかった場合は、[OK] (10.53.56.14) の下に表示されます。

ステップ 4 最初のノードで `utils dbreplication runtimestate` を入力して、データベース レプリケーションを再確立する試行の進行状況を監視します。

IM and Presence Service では、導入に複数のノードがある場合、データベース パブリッシャ ノードでこのコマンドを入力します。

すべてのノードで REPLICATION STATUS が **Connected** であり、REPLICATION SETUP 値が **(2) Setup Complete** であれば、レプリケーションは再確立されたと見なされます。

例：

```
admin: ユーティリティ dbreplication runtimestate DDB および Replication Services:
ALL RUNNING DB CLI Status: 他の dbreplication CLI が実行されていません... Cluster
Replication State: BROADCAST SYNC Completed on 1 servers at: 2013-09-26-15-18
Last Sync Result: SYNC COMPLETED 257 tables syncmonitorout of 257 Sync Errors:
NO ERRORS DB Version: ccm9_0_1_10000_9000 Number of レプリケート tables: 257
Repltimeout set to: 300sNewserver100 (2 サーバ) からのクラスタ詳細ビュー: レプリケー
ション複製を PING します。DBver& REPL. REPLICATION SETUP SERVER-NAME IP ADDRESS
(ミリ秒) RPC? STATUS QUEUE TABLES LOOP? (RTMT) & details -----
-----
server1 100.10.10.201 0.038 Yes Connected 0 match Yes (2) PUB Setup Completed
server2 100.10.10.202 0.248 Yes Connected 0 match Yes (2) Setup Completed
server3 100.10.10.203 0.248 Yes Connected 0 match Yes (2) Setup Completed
server4 100.10.10.204 0.248 Yes Connected 0
```

- レプリケーションが再確立された場合、ノード名の変更を確認する手順をもう一度実行し、新しいノード名が正常に複製されたことを検証します。
- レプリケーションが回復しない場合は、シスコのサポート担当者に連絡してこの問題を解決してください。

注意 データベース レプリケーションが切断されている場合は、これより先に進まないでください。

データベース レプリケーションのリセット

レプリケーションがクラスタのノードに設定されていない場合は、データベース レプリケーションをリセットします。コマンドライン インターフェイス (CLI) を使用してデータベース レプリケーションをリセットできます。

始める前に

クラスタにあるすべてのノードでデータベースレプリケーションのステータスを確認します。Replication Setup (RTMT) & Details に 2 の値が表示されていることを確認します。この値が 2 以外になっている場合は、データベースのレプリケーションに何らかの問題があるので、ノードのレプリケーションをリセットする必要があります。

手順

-
- ステップ 1** クラスタ内のノードでレプリケーションをリセットします。次のいずれかを実行します。
- a) Unified Communications Manager の場合は、`utils db replication reset all` と入力します。
いずれかの Cisco Unified Communications Manager ノードでこの CLI コマンドを実行する前に、まずリセットされているすべてのサブスクリバ ノードで、次にパブリッシャ サーバで `utils dbreplication stop` コマンドを実行します。詳細については、『*Command Line Interface Guide for Cisco Unified Communications Solutions*』を参照してください。
 - b) IM and Presence Service の場合は、データベースパブリッシャ ノードで `utils db replication reset all` と入力し、クラスタ内のすべての IM and Presence Service ノードをリセットします。
- ヒント** `all` の代わりに、特定のホスト名を入力して、そのノードだけのデータベースレプリケーションをリセットすることができます。詳細については、『*Command Line Interface Guide for Cisco Unified Communications Solutions*』を参照してください。
- ステップ 2** データベースレプリケーションのステータスを調べるには、`utils dbreplication runtimestate` と入力します。
IM and Presence Service の場合は、IM and Presence データベースパブリッシャ ノードで CLI コマンドを実行します。
-

ネットワークをトラブルシューティング

コマンドラインインターフェイス (CLI) を使用して、ノードのネットワークの問題をトラブルシューティングできます。

手順

-
- ステップ 1** ネットワーク設定を確認するために、`show network eth0 [detail]` を入力します。
- ステップ 2** フィールドのいずれかが欠落している場合は、ネットワークインターフェイスをリセットします。
- a) `set network status eth0 down` を入力します。
 - b) `set network status eth0 up` を入力します。

- ステップ 3** IP アドレス、マスク、およびゲートウェイを確認します。
これらの値がネットワーク全体で一意であることを確認します。

ネットワーク タイム プロトコル (NTP) のトラブルシューティング

サブスクライバノードにおける NTP のトラブルシューティング

コマンドラインインターフェイス (CLI) を使用して、サブスクライバノードの Network Time Protocol (NTP) の問題をトラブルシューティングできます。

手順

- ステップ 1** `show network eth0 [detail]` を入力して、ネットワーク設定を確認します。
ステップ 2 `utils ntp status` を入力して、NTP の状態を確認します。
ステップ 3 `utils ntp restart` を入力して、NTP を再起動します。
ステップ 4 `show network cluster` を入力して、ネットワークのクラスタを確認します。

誤ったパブリッシャ情報が出力に表示される場合は、`set network cluster publisher [hostname/IP_address]` CLI コマンドを使用して、パブリッシャをリセットします。

パブリッシャ ノードにおける NTP のトラブルシューティング

コマンドラインインターフェイス (CLI) を使用して、パブリッシャ ノードのネットワーク タイム プロトコル (NTP) の問題をトラブルシューティングできます。

手順

	コマンドまたはアクション	目的
ステップ 1	<code>show network eth0 [detail]</code> を入力して、ネットワーク設定を確認します。	
ステップ 2	<code>utils ntp status</code> を入力して、NTP の状態を確認します。	
ステップ 3	<code>utils ntp restart</code> を入力して、NTP を再起動します。	

	コマンドまたはアクション	目的
ステップ 4	<code>utils ntp server list</code> を入力して、NTP サーバを確認します。	NTP サーバを追加または削除するには、 <code>utils ntp server [add/delete]</code> CLI コマンドを使用します。



第 **VIII** 部

ディザスタリカバリ

- システムのバックアップ (487 ページ)
- システムの復元 (501 ページ)



第 34 章

システムのバックアップ

- [バックアップの概要 \(487 ページ\)](#)
- [バックアップの前提条件 \(489 ページ\)](#)
- [バックアップタスクフロー \(490 ページ\)](#)
- [バックアップの連携動作と制約事項 \(496 ページ\)](#)

バックアップの概要

定期的にバックアップを行うことを推奨します。ディザスタ リカバリ システム (DRS) を使用して、クラスタ内のすべてのサーバのデータを完全にバックアップできます。自動バックアップをセットアップすることも、任意の時点でバックアップを起動することもできます。

ディザスタ リカバリ システムで実行するバックアップは、クラスタ レベルであり、Cisco Unified Communications Manager クラスタ内のすべてのサーバのバックアップを 1 箇所に集め、バックアップデータを物理的なストレージデバイスにアーカイブします。バックアップファイルは暗号化され、システム ソフトウェアによってだけ開くことができます。

DRS は、プラットフォームのバックアップ/復元の一環として、独自の設定 (バックアップ デバイス設定およびスケジュール設定) を復元します。DRS は drfDevice.xml ファイルと drfSchedule.xml ファイルをバックアップおよび復元します。これらのファイルとともにサーバを復元するときは、DRS バックアップ デバイスおよびスケジュールを再設定する必要があります。

システムデータを復元するときには、クラスタ内のどのノードを復元するかを選択できます。

ディザスタ リカバリ システムには、次の機能があります。

- バックアップおよび復元タスクを実行するためのユーザ インターフェイス。
- バックアップ機能を実行するための分散システム アーキテクチャ。
- スケジュール バックアップまたは手動 (ユーザが起動する) バックアップ。
- リモート SFTP サーバへのバックアップのアーカイブ。

表に、ディザスタリカバリ システム (DRS) によるバックアップ/復元が可能な機能とコンポーネントを示します。各機能を選択すると、各機能のすべてのコンポーネントが自動的にバックアップされます。

表 85 : Cisco Unified CM の機能とコンポーネント

機能	コンポーネント
CCM : Unified Communications Manager	Unified Communications Manager データベース
	プラットフォーム
	サービサビリティ
	保留音 (MOH)
	Cisco Emergency Responder
	Bulk Tool (BAT)
	設定
	電話デバイス ファイル (TFTP)
	syslogagt (SNMP syslog エージェント)
	cdpagent (SNMP cdp エージェント)
	tct (トレース収集ツール)
	コール詳細レコード (CDR)
	CDR Reporting and Analysis (CAR)

表 86: IM and Presence の機能とコンポーネント

機能	コンポーネント
IM and Presence Service	IM and Presence データベース
	syslogagt (SNMP syslog エージェント)
	cdpagent (SNMP cdp エージェント)
	Platform
	レポーター (有用性レポーター)
	CUP SIP プロキシ
	XCP
	CLM
	Bulk Tool (BAT)
	設定
	tct (トレース収集ツール)

バックアップの前提条件

- バージョンの要件を満たしていることを確認してください。
 - すべての Cisco Unified Communications Manager クラスタ ノードは、同じバージョンの Cisco Unified Communications Manager アプリケーションを実行している必要があります。
 - すべての IM and Presence Service クラスタ ノードは、同じバージョンの IM and Presence Service アプリケーションを実行している必要があります。
 - バックアップ ファイルに保存されているソフトウェア バージョンが、クラスタ ノードで実行されるバージョンと同じでなければなりません。

バージョンの文字列全体が一致している必要があります。たとえば、IM and Presence データベースパブリッシャノードがバージョン 11.5.1.10000-1 の場合、すべての IM and Presence サブスクリバノードは 11.5.1.10000-1 であり、バックアップファイルに保存されているバージョンも 11.5.1.10000-1 でなければなりません。現在のバージョンと一致しないバックアップファイルからシステムを復元しようすると、復元は失敗します。バックアップファイルに保存されているバージョンが、クラスタノードで実行されているバージョンと一致するよう、ソフトウェアバージョンをアップグレードしたら常にシステムをバックアップするようにしてください。

- DRS 暗号化は、クラスタセキュリティパスワードに依存することに留意してください。バックアップの実行中に、DRS は暗号化のためにランダムパスワードを生成し、そのランダムパスワードをクラスタセキュリティパスワードを使用して暗号化します。バックアップを実行した後、復元を行うまでの間にクラスタセキュリティパスワードが変更された場合、そのバックアップファイルを使用してシステムを復元するには、バックアップを実行した時点でのパスワードを把握していなければなりません。あるいは、セキュリティパスワードを変更/リセットした直後にバックアップを作成するようにしてください。
- リモートデバイスをバックアップする必要がある場合は、必ず SFTP サーバを設定する必要があります。利用可能な SFTP サーバの詳細については、次の項を参照してください。
[リモートバックアップ用 SFTP サーバ \(497 ページ\)](#)

バックアップタスクフロー

次のタスクを実行して、バックアップを設定して実行します。バックアップの実行中は OS 管理タスクを実行しないでください。これは、ディザスタリカバリシステムがプラットフォーム API をロックすることにより、すべての OS 管理要求をブロックするためです。ただし、CLI ベースのアップグレードコマンドしかプラットフォーム API ロッキングパッケージを使用しないため、ディザスタリカバリシステムはほとんどの CLI コマンドを妨害しません。

手順

	コマンドまたはアクション	目的
ステップ 1	バックアップデバイスの設定 (491 ページ)	データをバックアップするデバイスを指定します。
ステップ 2	バックアップファイルのサイズの予測 (492 ページ)	SFTP デバイス上で作成されるバックアップファイルのサイズを見積もります。
ステップ 3	次のいずれかのオプションを選択します。 <ul style="list-style-type: none"> • スケジュールバックアップの設定 (493 ページ) • 手動バックアップの開始 (494 ページ) 	スケジュールに従ってデータをバックアップするためのバックアップスケジュールを作成します。 または、手動バックアップを実行します。
ステップ 4	現在のバックアップステータスの表示 (495 ページ)	これはオプションです。バックアップのステータスをチェックします。バックアップの実行中、現在のバックアップジョブのステータスを確認できます。
ステップ 5	バックアップ履歴の表示 (496 ページ)	これはオプションです。バックアップ履歴の表示

バックアップ デバイスの設定

最大 10 個のバックアップ デバイスを設定できます。バックアップ ファイルを保存する場所を設定するには、次の手順を実行します。

始める前に

- バックアップ ファイルを保存するために SFTP サーバにディレクトリ パスへの書き込みアクセス権があることを確認します。
- DRS マスターエージェントがバックアップ デバイスの設定を検証するときに、ユーザ名、パスワード、サーバ名とディレクトリ パスが有効であることを確認します。



(注) バックアップはネットワークトラフィックが少なくなる時間帯にスケジューリングしてください。

手順

ステップ 1 ディザスタリカバリ システムから、[バックアップ (Backup)] > [バックアップ デバイス (Backup Device)] の順に選択します。

ステップ 2 [バックアップ デバイス リスト (Backup Device List)] ウィンドウで、次のいずれかを実行します。

- 新しいデバイスを設定するには、[新規追加 (Add New)] をクリックします。
- 既存のバックアップ デバイスを編集するには、検索条件を入力し、[検索 (Find)]、次に [選択項目の編集 (Edit Selected)] をクリックします。
- バックアップ デバイスを削除するには、[バックアップ デバイス (Backup Device)] リストでバックアップ デバイスを選択してから [選択項目の削除 (Delete Selected)] をクリックします。

バックアップ スケジュールにバックアップ デバイスとして設定されているバックアップ デバイスは削除できません。

ステップ 3 [バックアップ デバイス名 (Backup device name)] フィールドにバックアップ名を入力します。バックアップ デバイス名には、英数字、スペース ()、ダッシュ (-)、およびアンダースコア (_) だけを使用します。それ以外の文字は使用しないでください。

ステップ 4 [接続先の選択 (Select Destination)] 領域の [ネットワーク ディレクトリ (Network Directory)] で、次を実行します。

- [ホスト名/IP アドレス (Host name/IP Address)] フィールドに、ネットワーク サーバのホスト名または IP アドレスを入力します。
- [パス名 (Path name)] フィールドに、バックアップ ファイルを格納するディレクトリ パスを入力します。

- [ユーザ名 (User name)] フィールドに、有効なユーザ名を入力します。
- [パスワード (Password)] フィールドに、有効なパスワードを入力します。
- [ネットワーク ディレクトリに保存するバックアップ数 (Number of backups to store on Network Directory)] ドロップダウン リストから、バックアップの必要数を選択します。

ステップ 5 [保存 (Save)] をクリックします。

次のタスク

[バックアップファイルのサイズの予測 \(492 ページ\)](#)

バックアップファイルのサイズの予測

1 つまたは複数の選択した機能のバックアップ履歴が存在する場合に限り、Cisco Unified Communications Manager は、バックアップ tar のサイズを予測します。

計算されたサイズは正確な値ではなく、バックアップ tar の予測サイズです。サイズは前のバックアップの実際のバックアップサイズに基づいて計算され、設定が前回のバックアップ以降変更された場合は異なることがあります。

この手順は、前回のバックアップが存在する場合にのみ使用でき、初めてシステムをバックアップする場合は使用できません。

SFTP デバイスに保存されているバックアップ tar のサイズを予測するには、次の手順に従ってください。

手順

-
- ステップ 1 ディザスタリカバリシステムから、[バックアップ (Backup)] > [手動バックアップ (Manual Backup)] の順に選択します。
 - ステップ 2 [機能の選択 (Select Features)] 領域でバックアップする機能を選択します。
 - ステップ 3 選択した機能のバックアップの予測サイズを表示するには、[サイズの予測 (Estimate Size)] を選択します。

次のタスク

システムをバックアップするには、次のいずれかの手順を実行します。

- [スケジュールバックアップの設定 \(493 ページ\)](#)
- [手動バックアップの開始 \(494 ページ\)](#)

スケジュール バックアップの設定

最大 10 個のバックアップ スケジュールを作成できます。各バックアップ スケジュールには、自動バックアップのスケジュール、バックアップする機能セット、保存場所など、独自のプロパティがあります。

バックアップ .tar ファイルはランダムに生成されるパスワードで暗号化されるということに注意してください。このパスワードは、クラスタセキュリティ パスワードで暗号化され、バックアップ .tar ファイルとともに保存されます。このセキュリティパスワードは忘れないように記憶しておくか、またはセキュリティ パスワードを変更またはリセットしたらすぐにバックアップを作成する必要があります。



注意 コール処理が中断してサービスに影響が及ばないように、バックアップはオフピーク時間中にスケジュールしてください。

始める前に

[バックアップ デバイスの設定 \(491 ページ\)](#)

手順

- ステップ 1** ディザスタリカバリ システムで、[バックアップ スケジューラ (Backup Scheduler)] を選択します。
- ステップ 2** [スケジュール リスト (Schedule List)] ウィンドウで、新規スケジュールを追加するか、または既存のスケジュールを編集します。
 - 新規スケジュールを作成するには、[新規追加 (Add New)] をクリックします。
 - 既存のスケジュールを設定するには、[スケジュール リスト (Schedule List)] 列でその名前をクリックします。
- ステップ 3** [スケジューラ (scheduler)] ウィンドウで、[スケジュール名 (Schedule Name)] フィールドにスケジュール名を入力します。

(注) デフォルトのスケジュールの名前は変更できません。
- ステップ 4** [バックアップ デバイスの選択 (Select Backup Device)] 領域でバックアップ デバイスを選択します。
- ステップ 5** [機能の選択 (Select Features)] 領域でバックアップする機能を選択します。少なくとも 1 つの機能を選択する必要があります。
- ステップ 6** [バックアップの開始時刻 (Start Backup at)] 領域でバックアップを開始する日付と時刻を選択します。
- ステップ 7** [頻度 (Frequency)] 領域でバックアップを行う頻度を選択します。頻度は、[一度 (Once)]、[日次 (Daily)]、[週次 (Weekly)]、[月次 (Monthly)] に設定できます。[週次 (Weekly)] を選択した場合は、バックアップを行う週の曜日も選択できます。

ヒント バックアップ頻度を火曜日から土曜日までの [週次 (Weekly)] に設定するには、[デフォルトの設定 (Set Default)] をクリックします。

ステップ 8 これらの設定を更新するには、[保存 (Save)] をクリックします。

ステップ 9 次のいずれかのオプションを選択します。

- 選択したスケジュールをイネーブルにするには、[選択されたスケジュールの有効化 (Enable Selected Schedules)] をクリックします。
- 選択したスケジュールをディセーブルにするには、[選択されたスケジュールの無効化 (Disable Selected Schedules)] をクリックします。
- 選択したスケジュールを削除するには、[選択項目の削除 (Delete Selected)] をクリックします。

ステップ 10 スケジュールを有効にするには、[スケジュールの有効化 (Enable Schedule)] をクリックします。

設定した時刻になると自動的に次のバックアップが実行されます。

- (注) クラスタ内のすべてのサーバが、同じバージョンの Cisco Unified Communications Manager または Cisco IM and Presence サービスを実行し、ネットワークから到達可能であることを確認します。スケジュールされたバックアップの時刻にサーバに到達できないと、そのサーバはバックアップされません。

次のタスク

次の手順を実行します。

- [バックアップ ファイルのサイズの予測 \(492 ページ\)](#)
- (省略可) [現在のバックアップ ステータスの表示 \(495 ページ\)](#)

手動バックアップの開始

始める前に

- バックアップ ファイルの格納場所としてネットワーク デバイスを使用していることを確認します。Unified Communications Manager の仮想化展開では、テープドライブによるバックアップ ファイルの保存はサポートされません。
- Cisco Unified Communications Manager または IM and Presence Service のインストールされているバージョンが、すべてのクラスタ ノードで同じであることを確認します。
- バックアップ プロセスは、リモート サーバに利用可能な容量がないためや、ネットワーク接続が中断されたために失敗することがあります。バックアップが失敗する原因となった問題に対処した後、新規のバックアップを開始する必要があります。

- ネットワークの中断がないことを確認してください。
- [バックアップ デバイスの設定 \(491 ページ\)](#)
- [バックアップ ファイルのサイズの予測 \(492 ページ\)](#)
- クラスタ セキュリティ パスワードのレコードがあることを確認します。このバックアップの完了後に、クラスタ セキュリティ パスワードを変更した場合は、パスワードを認識している必要があります。パスワードを認識していないと、バックアップファイルを使用してシステムを復元できなくなります。



- (注) バックアップが実行されている間は、Disaster Recovery System がプラットフォーム API をロックしてすべての要求をブロックするため、Cisco Unified OS の管理または Cisco Unified IM and Presence OS の管理でタスクを実行することはできません。ただし、ディザスタリカバリ システムは、CLI ベースのアップグレード コマンドだけがプラットフォーム API ロッキング パッケージを使用するため、ほとんどの CLI コマンドをブロックしません。

手順

- ステップ 1** ディザスタリカバリ システムから、[**バックアップ (Backup)**] > [**手動バックアップ (Manual Backup)**] の順に選択します。
- ステップ 2** [手動バックアップ (Manual Backup)] ウィンドウで、[**バックアップデバイス名 (Backup Device Name)**] 領域を選択します。
- ステップ 3** [機能の選択 (Select Features)] 領域から機能を選択します。
- ステップ 4** [バックアップの開始 (Start Backup)] をクリックします。

次のタスク

(省略可) [現在のバックアップステータスの表示 \(495 ページ\)](#)

現在のバックアップステータスの表示

現在のバックアップ ジョブのステータスを確認するには、次の手順を実行します。



- 注意** リモート サーバへのバックアップが 20 時間以内に完了しないとバックアップセッションがタイムアウトするため、新規バックアップを開始する必要があります。

手順

- ステップ1** ディザスタリカバリ システムから、[バックアップ (Backup)] > [現在のステータス (Current Status)] の順に選択します。
- ステップ2** バックアップ ログ ファイルを表示するには、ログファイル名リンクをクリックします。
- ステップ3** 現在のバックアップをキャンセルするには、[バックアップのキャンセル (Cancel Backup)] をクリックします。
- (注) 現在のコンポーネントがバックアップ操作を完了した後、バックアップがキャンセルされます。
-

次のタスク

[バックアップ履歴の表示 \(496 ページ\)](#)

バックアップ履歴の表示

バックアップ履歴を参照するには、次の手順を実行します。

手順

- ステップ1** ディザスタリカバリ システムから、[バックアップ (Backup)] > [履歴 (History)] の順に選択します。
- ステップ2** [バックアップ履歴 (Backup History)] ウィンドウで、ファイル名、バックアップ デバイス、完了日、結果、バージョン、バックアップされている機能、失敗した機能など、実行したバックアップを表示できます。
- (注) [バックアップ履歴 (Backup History)] ウィンドウには、最新の 20 個のバックアップジョブだけが表示されます。
-

バックアップの連携動作と制約事項

- [バックアップの制約事項 \(497 ページ\)](#)

バックアップの制約事項

バックアップには、次の制約事項が適用されます。

表 87: バックアップの制約事項

制限事項	説明
クラスタセキュリティパスワード	<p>クラスタセキュリティパスワードを変更したら、必ずバックアップを実行することを推奨します。</p> <p>バックアップ暗号化では、バックアップファイルのデータを暗号化する際にクラスタセキュリティパスワードを使用します。バックアップファイルの作成後にクラスタセキュリティパスワードを編集すると、古いパスワードを忘れてしまった場合に、そのバックアップファイルを使用してデータを復元できなくなります。</p>
証明書の管理	<p>ディザスタリカバリシステム (DRS) は、マスターエージェントとローカルエージェントとの間で SSL ベースの通信を使用して、Cisco Unified Communications Manager クラスタ ノード間のデータの認証および暗号化を行います。DRS は、IPSec 証明書を使用して、公開キー/秘密キーの暗号化を行います。証明書管理ページから IPSEC 信頼ストア (hostname.pem) ファイルを削除すると、DRS が想定どおりに機能しなくなることにご注意してください。IPSEC 信頼ファイルを手動で削除するときは、IPSEC 証明書を IPSEC 信頼に必ずアップロードしてください。詳細については、http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html にある『Security Guide for Cisco Unified Communications Manager』の「証明書管理」の項を参照してください。</p>

リモートバックアップ用 SFTP サーバ

データをネットワーク上のリモートデバイスにバックアップするには、SFTP サーバを用意して必要な設定を行う必要があります。シスコは内部テストでは、Cisco TAC にサポートされている、シスコ提供の Cisco Prime Collaboration Deployment (PCD) 上で SFTP サーバを使用します。SFTP サーバ オプションの概要については、次の表を参照してください。

以下の表示に記載されている情報を参考に、システムで使用する SFTP サーバソリューションを決定してください。

表 88: SFTP サーバ情報

SFTP サーバ	情報
Cisco Prime Collaboration Deployment の SFTP サーバ	<p>このサーバはシスコが提供およびテストした SFTP サーバのみであり、Cisco TAC がサポートします。</p> <p>バージョンの互換性は、使用している Unified Communications Manager および Cisco Prime Collaboration Deployment のバージョンに依存します。バージョン (SFTP) または Unified Communications Manager をアップグレードする前に、『Cisco Prime Collaboration Deployment Administration Guide』を参照して、互換性のあるバージョンであることを確認してください。</p>
テクノロジーパートナーの SFTP サーバ	<p>これらのサーバはサードパーティが提供およびテストしたものです。バージョンの互換性は、サードパーティによるテストに依存します。テクノロジーパートナーの SFTP サーバまたは Unified Communications Manager をアップグレードする場合、テクノロジーパートナーのページで、互換性のあるバージョンを確認してください。</p> <p>https://marketplace.cisco.com</p>
他のサードパーティの SFTP サーバ	<p>これらのサーバはサードパーティが提供するものであり、Cisco TAC はこれらのサーバを正式にサポートしていません。</p> <p>バージョンの互換性は、SFTP バージョンと Unified Communications Manager バージョンの互換性を確立するためのベストエフォートに基づきます。</p> <p>(注) これらの製品がシスコでテストされていない場合、シスコはその機能を保証することができません。Cisco TAC は、これらの製品をサポートしていません。完全にテストされてサポートされる SFTP ソリューションとしては、Cisco Prime Collaboration Deployment またはテクノロジーパートナーの SFTP サーバを利用してください。</p>

暗号サポート

Unified Communications Manager 11.5 では、Unified Communications Manager は SFTP 接続用に次の CBC および CRT 暗号をアドバタイズします。

- aes128-cbc
- 3des-cbc
- aes128-ctr
- aes192-ctr

- aes256-ctr



(注) Unified Communications Manager との通信のために、バックアップ SFTP サーバがこれらの暗号のいずれかをサポートしていることを確認してください。

Unified Communications Manager 12.0 リリース以降では、CBC 暗号はサポートされていません。Unified Communications Manager は、次の CTR 暗号のみをサポートおよびアドバタイズします。

- aes256-ctr
- aes128-ctr
- aes192-ctr



(注) バックアップ SFTP サーバが Unified Communications Manager との通信のためにこれらの CTR 暗号のいずれかをサポートしていることを確認します。



第 35 章

システムの復元

- 復元の概要 (501 ページ)
- 復元的前提条件 (502 ページ)
- 復元タスク フロー (503 ページ)
- データ認証 (514 ページ)
- アラームおよびメッセージ (516 ページ)
- ライセンス予約 (519 ページ)
- ライセンス情報 (520 ページ)
- 復元の連携動作と制約事項 (522 ページ)
- トラブルシューティング (523 ページ)

復元の概要

ディザスタリカバリシステム (DRS) には、システムを復元するプロセスを実行するためのガイドとなるウィザードが用意されています。

バックアップファイルは暗号化されており、それらを開いてデータを復元できるのは DRS システムのみです。ディザスタリカバリシステムには、次の機能があります。

- 復元タスクを実行するためのユーザインターフェイス。
- 復元機能を実行するための分散システムアーキテクチャ。

マスター エージェント

クラスタの各ノードで自動的にマスター エージェント サービスが起動されますが、マスター エージェントはパブリッシャ ノード上でのみ機能します。サブスクリバノード上のマスター エージェントは、何の機能も実行しません。

ローカル エージェント

サーバには、バックアップおよび復元機能を実行するローカルエージェントが搭載されていません。

マスターエージェントを含むノードをはじめ、Cisco Unified Communications Manager クラスタ内の各ノードには、バックアップおよび復元機能を実行するために独自のローカルエージェントが必要です。



(注) デフォルトでは、ローカルエージェントは IM and Presence ノードをはじめ、クラスタ内の各ノードで自動的に起動されます。

復元の前提条件

- バージョンの要件を満たしていることを確認してください。
 - すべての Cisco Unified Communications Manager クラスタ ノードは、同じバージョンの Cisco Unified Communications Manager アプリケーションを実行している必要があります。
 - すべての IM and Presence Service クラスタ ノードは、同じバージョンの IM and Presence Service アプリケーションを実行している必要があります。
 - バックアップ ファイルに保存されているバージョンが、クラスタ ノードで実行されるバージョンと同じでなければなりません。

バージョンの文字列全体が一致している必要があります。たとえば、IM and Presence データベースパブリッシャ ノードがバージョン 11.5.1.10000-1 の場合、すべての IM and Presence サブスクリバ ノードは 11.5.1.10000-1 であり、バックアップファイルに保存されているバージョンも 11.5.1.10000-1 でなければなりません。現在のバージョンと一致しないバックアップファイルからシステムを復元しようすると、復元は失敗します。

- サーバの IP アドレス、ホスト名、DNS 設定および導入タイプが、バックアップファイルに保存されている IP アドレス、ホスト名、DNS 設定および導入タイプと一致していることを確認します。
- バックアップを実行した後にクラスタセキュリティ パスワードを変更した場合、元のパスワードの記録を記録しておきます。元のパスワードが分からなければ、復元は失敗します。
- クラスタで IPsec ポリシーが有効になっている場合は、復元操作を開始する前に無効にしてください。

復元後に SAML SSO を再度有効にする



重要 このセクションは、リリース 12.5(1)SU7 にのみ適用されます。

DRS を使用してシステムを復元した後、クラスタ内のいずれかのノードで SAML SSO が断続的に無効化されることがあります。影響を受けるノードで SAML SSO を再度有効にするには、以下を実行する必要があります：

1. Cisco Unified CM の管理で、[システム (System)] > [SAML シングルサインオン (SAML Single Sign-On)] を選択します。
2. [SSO テストを実行 (Run SSO Test)] をクリックします。
3. [SSO のテストに成功しました! (SSO Test Succeeded!)] というメッセージが表示されたら、ブラウザウィンドウを閉じ、[終了 (Finish)] をクリックします。



(注) SAML SSO を再度有効にするプロセス中に Cisco Tomcat が再起動します。SAML SSO がすでに有効になっているノードには影響しません。

復元タスク フロー

復元プロセス中、[Cisco Unified CM の管理 (Cisco Unified Communications Manager OS Administration)] または [Cisco Unified CM IM and Presence OS の管理 (Cisco Unified IM and Presence OS Administration)] に関するタスクを実行しないでください。

手順

	コマンドまたはアクション	目的
ステップ 1	最初のノードのみの復元 (504 ページ)	(オプション) クラスタ内の最初のパブリッシャノードだけを復元する場合は、この手順を使用します。
ステップ 2	後続クラスタ ノードの復元 (506 ページ)	(オプション) クラスタ内のサブスクライバノードを復元する場合は、この手順を使用します。
ステップ 3	パブリッシャの再構築後の1回のステップでのクラスタの復元 (508 ページ)	(オプション) パブリッシャがすでに再構築されている場合、1回のステップでクラスタ全体を復元するには、次の手順に従ってください。
ステップ 4	クラスタ全体の復元 (510 ページ)	(オプション) パブリッシャノードを含む、クラスタ内のすべてのノードを復元

	コマンドまたはアクション	目的
		元するには、この手順を使用します。主要なハードドライブで障害またはアップグレードが発生した場合や、ハードドライブを移行する場合には、クラスタ内のすべてのノードの再構築が必要になる場合があります。
ステップ 5	前回正常起動時の設定へのノードまたはクラスタの復元 (511 ページ)	(オプション) 前回正常起動時の設定にノードを復元する場合に限り、この手順を使用します。ハードドライブ障害やその他のハードウェア障害の後には使用しないでください。
ステップ 6	ノードの再起動 (512 ページ)	ノードを再起動するには、この手順を使用します。
ステップ 7	復元ジョブステータスのチェック (513 ページ)	(オプション) 復元ジョブステータスを確認するには、この手順を使用します。
ステップ 8	復元履歴の表示 (513 ページ)	(オプション) 復元履歴を表示するには、この手順を使用します。

最初のノードのみの復元

再構築後に最初のノードを復元する場合は、バックアップデバイスを設定する必要があります。

この手順は、Cisco Unified Communications Manager の最初のノード (パブリッシャ ノードとも呼ばれます) に対して実行できます。その他の Cisco Unified Communications Manager ノードおよびすべての IM and Presence サービス ノードは、セカンダリ ノードまたはサブスクリバと見なされます。

始める前に

クラスタ内に IM and Presence サービス ノードがある場合は、最初のノードを復元するときに、ノードが実行されており、アクセス可能であることを確認してください。これは、この手順の実行中に有効なバックアップ ファイルを見つけるために必須です。

手順

- ステップ 1** ディザスタリカバリ システムから、[復元 (Restore)] > [復元ウィザード (Restore Wizard)] を選択します。

- ステップ 2** [復元ウィザード ステップ 1 (Restore Wizard Step 1)] ウィンドウの [バックアップ デバイスの選択 (Select Backup Device)] 領域で、復元する適切なバックアップ デバイスを選択します。
- ステップ 3** [次へ (Next)] をクリックします。
- ステップ 4** [復元ウィザード ステップ 2 (Restore Wizard Step 2)] ウィンドウで、復元するバックアップ ファイルを選択します。
- (注) バックアップ ファイル名から、バックアップ ファイルが作成された日付と時刻がわかります。
- ステップ 5** [次へ (Next)] をクリックします。
- ステップ 6** [復元ウィザード ステップ 3 (Restore Wizard Step 3)] ウィンドウで、[次へ (Next)] をクリックします。
- ステップ 7** 復元する機能を選択します。
- (注) バックアップ 対象として選択した機能が表示されます。
- ステップ 8** [次へ (Next)] をクリックします。[復元ウィザード ステップ 4 (Restore Wizard Step 4)] ウィンドウが表示されます。
- ステップ 9** ファイル整合性チェックを実行する場合は、[SHA1 メッセージダイジェストを使用してファイル整合性チェックを実行する (Select the Perform file integrity check using SHA1 Message Digest)] チェックボックスをオンにします。
- (注) ファイル整合性チェックは任意で、SFTP バックアップの場合にだけ必要です。
- ファイル整合性チェックの処理は CPU およびネットワーク帯域幅を大量に消費するため、復元プロセスの処理速度が低下します。
- FIPS モードでのメッセージダイジェスト検証にも SHA-1 を使用できます。SHA-1 は、デジタル署名に使用されない HMAC やランダムビット生成などのハッシュ関連アプリケーションでのすべての非デジタル署名の使用に許可されています。たとえば、SHA-1 は引き続きチェックサム の計算に使用できます。署名の生成と検証にのみ、SHA-1 は使用できません。
- ステップ 10** 復元するノードを選択します。
- ステップ 11** [復元 (Restore)] をクリックして、データを復元します。
- ステップ 12** [次へ (Next)] をクリックします。
- ステップ 13** 復元するノードの選択を求められたら、最初のノード (パブリッシャ) だけを選択します。
- 注意** このときに後続 (サブスクリバ) ノードは選択しないでください。復元を試みても失敗します。
- ステップ 14** (オプション) [サーバ名の選択 (Select Server Name)] ドロップダウンリストから、パブリッシャデータベース復元元のサブスクリバノードを選択します。選択したサブスクリバノードが稼働しており、クラスタに接続されていることを確認してください。ディザスタリカバリ システムでバックアップ ファイルのすべてのデータベース以外の情報が復元され、選択した後続ノードから最新のデータベースが取り出されます。

(注) このオプションは、選択したバックアップファイルに CCMDB データベース コンポーネントが含まれている場合にのみ表示されます。まず、パブリッシャノードだけが完全に復元されますが、ステップ 14 を実行し、後続のクラスタノードを再起動すると、ディザスタリカバリシステムはデータベースレプリケーションを実行し、完全にすべてのクラスタノードのデータベースが同期されます。これにより、すべてのクラスタノードに最新のデータを使用していることが保障されます。

ステップ 15 [復元 (Restore)] をクリックします。

ステップ 16 パブリッシャノードにデータが復元されます。復元するデータベースとコンポーネントのサイズによっては、復元が完了するまでに数時間かかることがあります。

(注) 最初のノードを復元すると、Cisco Unified Communications Manager データベース全体がクラスタに復元されます。そのため、復元しているノードの数とデータベースのサイズによっては、数時間かかることがあります。復元するデータベースとコンポーネントのサイズによっては、復元が完了するまでに数時間かかることがあります。

ステップ 17 [復元ステータス (Restore Status)] ウィンドウの [完了率 (Percentage Complete)] フィールドに 100% と表示されたら、サーバを再起動します。クラスタ内のすべてのノードの再起動は最初のノードのみへの復元の場合に必要となります。後続ノードを再起動する前に、必ず最初のノードを再起動してください。サーバの再起動方法については、「次の作業」の項を参照してください。

(注) Cisco Unified Communications Manager ノードだけを復元する場合は、Cisco Unified Communications Manager and IM and Presence Service サービスクラスタを再起動する必要があります。

IM and Presence サービスのパブリッシャノードのみを復元する場合は、IM and Presence サービスクラスタを再起動する必要があります。

次のタスク

- (オプション) 復元のステータスを表示するには、次を参照してください。 [復元ジョブステータスのチェック \(513 ページ\)](#)
- ノードを再起動するには、次を参照してください： [ノードの再起動 \(512 ページ\)](#)

後続クラスタノードの復元

この手順は、Cisco Unified Communications Manager のサブスクリバ (後続) ノードにのみ適用されます。インストールされる最初の Cisco Unified Communications Manager ノードはパブリッシャノードです。その他すべての Cisco Unified Communications Manager ノードおよびすべての IM and Presence サービス ノードはサブスクリバノードです。

クラスタ内の1つ以上の Cisco Unified Communications Manager サブスクリバノードを復元するには、次の手順に従います。

始める前に

復元操作を実行する場合は事前に、復元のホスト名、IP アドレス、DNS 設定、および配置タイプが、復元するバックアップファイルのホスト名、IP アドレス、DNS 設定、および配置タイプに一致することを確認します。ディザスタリカバリシステムでは、ホスト名、IP アドレス、DNS 設定、および配置タイプが異なると復元が行われません。

サーバにインストールされているソフトウェアのバージョンが復元するバックアップファイルのバージョンに一致することを確認します。ディザスタリカバリシステムは、一致するソフトウェアバージョンのみを復元操作でサポートします。再構築後に後続ノードを復元している場合は、バックアップデバイスを設定する必要があります。

手順

- ステップ 1** ディザスタリカバリシステムから、**[復元 (Restore)] > [復元ウィザード (Restore Wizard)]** を選択します。
- ステップ 2** **[復元ウィザードステップ 1 (Restore Wizard Step 1)]** ウィンドウの **[バックアップデバイスの選択 (Select Backup Device)]** 領域で、復元元のバックアップデバイスを選択します。
- ステップ 3** **[次へ (Next)]** をクリックします。
- ステップ 4** **[復元ウィザードステップ 2 (Restore Wizard Step 2)]** ウィンドウで、復元するバックアップファイルを選択します。
- ステップ 5** **[次へ (Next)]** をクリックします。
- ステップ 6** **[復元ウィザードステップ 3 (Restore Wizard Step 3)]** ウィンドウで、復元する機能を選択します。
(注) 選択したファイルにバックアップされた機能だけが表示されます。
- ステップ 7** **[次へ (Next)]** をクリックします。**[復元ウィザードステップ 4 (Restore Wizard Step 4)]** ウィンドウが表示されます。
- ステップ 8** **[復元ウィザードステップ 4 (Restore Wizard Step 4)]** ウィンドウで、復元するノードを選択するよう求められたら、後続ノードのみを選択します。
- ステップ 9** **[復元 (Restore)]** をクリックします。
- ステップ 10** 後続ノードにデータが復元されます。復元ステータスの確認方法については、「次の作業」の項を参照してください。
(注) 復元プロセス中、**[Cisco Unified CM の管理 (Cisco Unified Communications Manager Administration)]** または **[ユーザ オプション (User Options)]** に関するタスクを実行しないでください。
- ステップ 11** **[復元ステータス (Restore Status)]** ウィンドウの **[完了率 (Percentage Complete)]** フィールドに 100% と表示されたら、復元した 2 次サーバを再起動します。クラスタ内のすべてのノード

の再起動は最初のノードのみへの復元の場合に必要となります。後続ノードを再起動する前に、必ず最初のノードを再起動してください。サーバの再起動方法については、「次の作業」の項を参照してください。

- (注) 最初の IM and Presence サービス ノードが復元されたら、後続の IM and Presence Service ノードを再起動する前に、必ず最初の IM and Presence Service ノードを再起動してください。

次のタスク

- (オプション) 復元のステータスを表示するには、次を参照してください。 [復元ジョブステータスのチェック \(513 ページ\)](#)
- ノードを再起動するには、次を参照してください: [ノードの再起動 \(512 ページ\)](#)

パブリッシャの再構築後の1回のステップでのクラスタの復元

復元するデータベースとコンポーネントのサイズによっては、復元が完了するまでに数時間かかることがあります。パブリッシャがすでに再構築されている場合、または新しくインストールされた場合に、1回のステップでクラスタ全体を復元する場合は、次の手順に従います。

手順

- ステップ 1** ディザスタリカバリ システムから、**[復元 (Restore)] > [復元ウィザード (Restore Wizard)]** を選択します。
- ステップ 2** **[復元ウィザード ステップ 1 (Restore Wizard Step 1)]** ウィンドウの **[バックアップ デバイスの選択 (Select Backup Device)]** 領域で、復元するバックアップ デバイスを選択します。
- ステップ 3** **[次へ (Next)]** をクリックします。
- ステップ 4** **[復元ウィザード ステップ 2 (Restore Wizard Step 2)]** ウィンドウで、復元するバックアップ ファイルを選択します。
- バックアップファイル名から、バックアップファイルが作成された日付と時刻がわかります。クラスタ全体を復元するクラスタのバックアップ ファイルだけを選択します。
- ステップ 5** **[次へ (Next)]** をクリックします。
- ステップ 6** **[復元ウィザード ステップ 3 (Restore Wizard Step 3)]** ウィンドウで、復元する機能を選択します。
- 画面には、復元する機能のうち、バックアップ ファイルに保存された機能のみが表示されます。
- ステップ 7** **[次へ (Next)]** をクリックします。

ステップ 8 [復元ウィザード ステップ 4 (Restore Wizard Step 4)] ウィンドウで、[1 ステップでの復元 (One-Step Restore)] をクリックします。

このオプションは、復元対象として選択されたバックアップファイルがクラスタのバックアップファイルであり、復元対象として選択された機能に、パブリッシャとサブスクライバの両方のノードに登録された機能が含まれている場合にのみ、[復元ウィザード ステップ 4 (Restore Wizard Step 4)] ウィンドウに表示されます。詳細については、[最初のノードのみの復元 \(504 ページ\)](#) および [後続クラスタ ノードの復元 \(506 ページ\)](#) を参照してください。

(注) パブリッシャがクラスタ対応になりませんでした。1 ステップでの復元を開始できません (Publisher has failed to become cluster aware. Cannot start one-step restore) 」というステータス メッセージが表示されたら、パブリッシャ ノードを復元してからサブスクライバノードを復元する必要があります。詳細については、「[関連項目](#)」を参照してください。

このオプションでは、パブリッシャがクラスタ対応になり、そのためには5分かかります。このオプションをクリックすると、ステータスメッセージに「「パブリッシャがクラスタ対応になるまで5分間待機してください。この期間にバックアップまたは復元処理を開始しないでください。(Please wait for 5 minutes until Publisher becomes cluster aware and do not start any backup or restore activity in this time period.) 」」と表示されます。

この待ち時間の経過後に、パブリッシャがクラスタ対応になると、「「パブリッシャがクラスタ対応になりました」」が表示されます。サーバを選択し、[復元 (Restore)] をクリックしてクラスタ全体の復元を開始してください。(Please select the servers and click on Restore to start the restore of entire cluster) 」というステータスメッセージが表示されます。

この待ち時間の経過後、パブリッシャがクラスタ対応にならない場合、「パブリッシャがクラスタ対応にならなかったため、1 ステップでの復元を開始できません。通常の 2 ステップでの復元を実行してください。(Publisher has failed to become cluster aware. Cannot start one-step restore. Please go ahead and do a normal two-step restore.) 」というステータスメッセージが表示されます。クラスタ全体を2ステップ (パブリッシャとサブスクライバ) で復元するには、[最初のノードのみの復元 \(504 ページ\)](#) と [後続クラスタ ノードの復元 \(506 ページ\)](#) で説明する手順を実行してください。

ステップ 9 復元するノードの選択を求められたら、クラスタ内のすべてのノードを選択します。

最初のノードを復元すると、ディザスタリカバリ システムが自動的に後続ノードに Cisco Unified Communications Manager データベース (CCMDB) を復元します。そのため、復元しているノードの数とデータベースのサイズによっては、数時間かかることがあります。

ステップ 10 [復元 (Restore)] をクリックします。
クラスタ内のすべてのノードでデータが復元されます。

ステップ 11 [復元ステータス (Restore Status)] ウィンドウの [完了率 (Percentage Complete)] フィールドに 100% と表示されたら、サーバを再起動します。クラスタ内のすべてのノードの再起動は最初のノードのみへの復元の場合に必要となります。後続ノードを再起動する前に、必ず最初の

ノードを再起動してください。サーバの再起動方法については、「次の作業」の項を参照してください。

次のタスク

- (オプション) 復元のステータスを表示するには、次を参照してください。 [復元ジョブステータスのチェック \(513 ページ\)](#)
- ノードを再起動するには、次を参照してください： [ノードの再起動 \(512 ページ\)](#)

クラスタ全体の復元

主要なハード ドライブで障害またはアップグレードが発生した場合や、ハード ドライブを移行する場合には、クラスタ内のすべてのノードの再構築が必要です。クラスタ全体を復元するには、次の手順を実行します。

ネットワーク カードの交換やメモリの増設など他のほとんどのハードウェア アップグレードでは、次の手順を実行する必要はありません。

手順

- ステップ 1** ディザスタリカバリ システムから、**[復元 (Restore)] > [復元ウィザード (Restore Wizard)]** を選択します。
- ステップ 2** **[バックアップデバイスの選択 (Select Backup Device)]** エリアで、復元する適切なバックアップ デバイスを選択します。
- ステップ 3** **[次へ (Next)]** をクリックします。
- ステップ 4** **[復元ウィザード ステップ 2 (Restore Wizard Step 2)]** ウィンドウで、復元するバックアップ ファイルを選択します。
- (注) バックアップ ファイル名から、バックアップ ファイルが作成された日付と時刻がわかります。
- ステップ 5** **[次へ (Next)]** をクリックします。
- ステップ 6** **[復元ウィザード ステップ 3 (Restore Wizard Step 3)]** ウィンドウで、**[次へ (Next)]** をクリックします。
- ステップ 7** **[復元ウィザード ステップ 4 (Restore Wizard Step 4)]** ウィンドウで復元ノードの選択を求められたら、すべてのノードを選択します。
- ステップ 8** **[復元 (Restore)]** をクリックして、データを復元します。

最初のノードを復元すると、ディザスタリカバリ システムが自動的に後続ノードに Cisco Unified Communications Manager データベース (CCMDB) を復元します。そのため、ノードの数とデータベースのサイズによっては、最大数時間かかることがあります。

すべてのノードでデータが復元されます。

(注) 復元プロセス中、[Cisco Unified CM の管理 (Cisco Unified Communications Manager Administration)] または [ユーザ オプション (User Options)] に関するタスクを実行しないでください。

復元するデータベースとコンポーネントのサイズによっては、復元が完了するまでに数時間かかることがあります。

ステップ 9 復元プロセスが完了したら、サーバを再起動します。サーバの再起動方法の詳細については、「次の作業」セクションを参照してください。

(注) 必ず最初のノードを再起動してから、後続ノードを再起動してください。

最初のノードが再起動し、Cisco Unified Communications Manager の復元後のバージョンが実行されたら、後続ノードを再起動します。

ステップ 10 レプリケーションはクラスタのリポート後に自動的にセットアップされます。『*Command Line Interface Reference Guide for Cisco Unified Communications Solutions*』の説明に従って「utils dbreplication runtimestate」CLI コマンドを使用して、すべてのノードで [レプリケーション ステータス (Replication Status)] の値を確認します。各ノードの値は 2 になっているはずですが。

(注) クラスタのサイズによっては、後続ノードの再起動後に、後続ノードでのデータベース レプリケーションが完了するまでに時間がかかる場合があります。

ヒント レプリケーションが正しくセットアップされない場合は、『*Command Line Interface Reference Guide for Cisco Unified Communications Solutions*』の説明に従って「utils dbreplication rebuild」CLI コマンドを使用します。

次のタスク

- (オプション) 復元のステータスを表示するには、次を参照してください。 [復元ジョブステータスのチェック \(513 ページ\)](#)
- ノードを再起動するには、次を参照してください： [ノードの再起動 \(512 ページ\)](#)

前回正常起動時の設定へのノードまたはクラスタの復元

前回正常起動時の設定にノードまたはクラスタを復元するには、次の手順に従います。

始める前に

- 復元ファイルに、バックアップ ファイルで設定されているホスト名、IP アドレス、DNS 設定、および配置タイプが含まれていることを確認します。
- サーバにインストールされている Cisco Unified Communications Manager のバージョンが復元するバックアップ ファイルのバージョンに一致することを確認します。
- この手順は、前回正常起動時の設定にノードを復元する場合にのみ使用してください。

手順

-
- ステップ 1** ディザスタリカバリ システムから、**[復元 (Restore)] > [復元ウィザード (Restore Wizard)]** を選択します。
- ステップ 2** **[バックアップデバイスの選択 (Select Backup Device)]** 領域で、復元する適切なバックアップ デバイスを選択します。
- ステップ 3** **[次へ (Next)]** をクリックします。
- ステップ 4** **[復元ウィザード ステップ 2 (Restore Wizard Step 2)]** ウィンドウで、復元するバックアップ ファイルを選択します。
- (注) バックアップ ファイル名から、バックアップ ファイルが作成された日付と時刻がわかります。
- ステップ 5** **[次へ (Next)]** をクリックします。
- ステップ 6** **[復元ウィザード ステップ 3 (Restore Wizard Step 3)]** ウィンドウで、**[次へ (Next)]** をクリックします。
- ステップ 7** 復元ノードを選択するように求められたら、該当するノードを選択します。選択したノードにデータが復元されます。
- ステップ 8** クラスタ内のすべてのノードを再起動します。後続の Cisco Unified Communications Manager ノードを再起動する前に、最初の Cisco Unified Communications Manager ノードを再起動します。クラスタに Cisco IM and Presence ノードもある場合は、最初の Cisco IM and Presence ノードを再起動してから、後続の IM and Presence ノードを再起動します。詳細については、「次の作業」の項を参照してください。
-

ノードの再起動

データを復元したら、ノードを再起動する必要があります。

パブリッシャ ノード (最初のノード) を復元したら、最初にパブリッシャ ノードを再起動する必要があります。サブスクライバノードは必ず、パブリッシャ ノードが再起動し、ソフトウェアの復元されたバージョンを正常に実行し始めた後で再起動してください。



-
- (注) CUCM パブリッシャノードがオフラインの場合は、IM and Presence サブスクライバノードを再起動しないでください。このような場合、サブスクライバノードが CUCM パブリッシャに接続できないため、ノードサービスが起動しません。
-



-
- 注意** この手順を実行すると、システムが再起動し、一時的に使用できない状態になります。
-

再起動する必要があるクラスタ内のすべてのノードでこの手順を実行します。

手順

- ステップ 1 [Cisco Unified OS の管理 (Cisco Unified OS Administration)] から、[設定 (Settings)] > [バージョン (Version)] を選択します。
- ステップ 2 ノードを再起動するには、[再起動 (Restart)] をクリックします。
- ステップ 3 レプリケーションはクラスタのリブート後に自動的に設定されます。 **utils dbreplication runtimestate** CLI コマンドを使用して、すべてのノードで [レプリケーションステータス (Replication Status)] 値を確認します。各ノードの値は 2 になっているはずですが。CLI コマンドの詳細については、『Cisco Unified Communications (CallManager) Command References』を参照してください。

レプリケーションが正しくセットアップされない場合は、『*Command Line Reference Guide for Cisco Unified Communications Solutions*』の説明に従って **utils dbreplication reset** CLI コマンドを使用します。

(注) クラスタのサイズによっては、後続ノードの再起動後に、後続ノードでのデータベースレプリケーションが完了するまでに数時間かかる場合があります。

次のタスク

(オプション) 復元のステータスを表示するには、[復元ジョブステータスのチェック \(513 ページ\)](#) を参照してください。

復元ジョブステータスのチェック

次の手順に従って、復元ジョブステータスをチェックします。

手順

- ステップ 1 ディザスタリカバリシステムで、[復元 (Restore)] > [現在のステータス (Current Status)] を選択します。
- ステップ 2 [復元ステータス (Restore Status)] ウィンドウで、ログファイル名のリンクをクリックし、復元ステータスを表示します。

復元履歴の表示

復元履歴を参照するには、次の手順を実行します。

手順

-
- ステップ1 [Disaster Recovery System] で、[復元 (Restore)] > [履歴 (History)] を選択します。
- ステップ2 [復元履歴 (Restore History)] ウィンドウで、ファイル名、バックアップ デバイス、完了日、結果、バージョン、復元された機能、失敗した機能など、実行した復元を表示できます。
- [復元履歴 (Restore History)] ウィンドウには、最新の20個の復元ジョブだけが表示されます。
-

データ認証

トレース ファイル

トラブルシューティングを行う際、またはログの収集中には、トレースファイルの保存先として次の場所が使用されます。

マスター エージェント、GUI、各ローカル エージェント、および JSch ライブラリのトレースファイルは次の場所書き込まれます。

- マスター エージェントの場合、トレース ファイルは platform/drf/trace/drfMA0* にあります。
- 各ローカル エージェントの場合、トレース ファイルは platform/drf/trace/drfLA0* にあります。
- GUI の場合、トレース ファイルは platform/drf/trace/drfConfLib0* にあります。
- JSch の場合、トレース ファイルは platform/drf/trace/drfJSch* にあります。

詳細については、『*Command Line Interface Reference Guide for Cisco Unified Communications Solutions*』（<http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-command-reference-list.html>）を参照してください。

コマンドライン インターフェイス

ディザスタリカバリ システムでは、次の表に示すように、バックアップおよび復元機能のサブセットにコマンドラインからアクセスできます。これらのコマンドの内容とコマンドライン インターフェイスの使用法の詳細については、『*Command Line Interface (CLI) Reference Guide for Cisco Unified Presence*』（<http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-command-reference-list.html>）を参照してください。

表 89: ディザスタリカバリ システムのコマンドラインインターフェイス

コマンド	説明
utils disaster_recovery estimate_tar_size	SFTP/Local デバイスからのバックアップ tar の概算サイズを表示し、機能リストのパラメータを1つ要求します。
utils disaster_recovery backup	ディザスタリカバリ システムのインターフェイスに設定されている機能を使用して、手動バックアップを開始します。
utils disaster_recovery jschLogs	JSch ライブラリのロギングを有効または無効にします。
utils disaster_recovery restore	復元を開始します。復元するバックアップ場所、ファイル名、機能、およびノードを指定するためのパラメータが必要です。
utils disaster_recovery status	進行中のバックアップジョブまたは復元ジョブのステータスを表示します。
utils disaster_recovery show_backupfiles	既存のバックアップファイルを表示します。
utils disaster_recovery cancel_backup	進行中のバックアップジョブをキャンセルします。
utils disaster_recovery show_registration	現在設定されている登録を表示します。
utils disaster_recovery device add	ネットワーク デバイスを追加します。
utils disaster_recovery device delete	デバイスを削除します。
utils disaster_recovery device list	すべてのデバイスを一覧表示します。
utils disaster_recovery schedule add	スケジュールを追加します。
utils disaster_recovery schedule delete	スケジュールを削除します。
utils disaster_recovery schedule disable	スケジュールを無効にします。
utils disaster_recovery schedule enable	スケジュールを有効にします。
utils disaster_recovery schedule list	すべてのスケジュールを一覧表示します。
utils disaster_recovery backup	ディザスタリカバリ システムのインターフェイスに設定されている機能を使用して、手動バックアップを開始します。

コマンド	説明
utils disaster_recovery restore	復元を開始します。復元するバックアップ場所、ファイル名、機能、およびノードを指定するためのパラメータが必要です。
utils disaster_recovery status	進行中のバックアップ ジョブまたは復元ジョブのステータスを表示します。
utils disaster_recovery show_backupfiles	既存のバックアップ ファイルを表示します。
utils disaster_recovery cancel_backup	進行中のバックアップ ジョブをキャンセルします。
utils disaster_recovery show_registration	現在設定されている登録を表示します。

アラームおよびメッセージ

アラームおよびメッセージ

ディザスタリカバリシステムは、バックアップまたは復元手順の実行時に発生するさまざまなエラーのアラームを発行します。次の表に、ディザスタリカバリシステムのアラームの一覧を記載します。

表 90: ディザスタリカバリシステムのアラームとメッセージ

アラーム名	説明	説明
DRFBackupDeviceError	DRF バックアップ プロセスでデバイスへのアクセスに関する問題が発生しています。	DRS バックアップ プロセスへのアクセス中にエラーしました。
DRFBackupFailure	シスコ DRF バックアップ プロセスが失敗しました。	DRS バックアップ プロセスが発生しました。
DRFBackupInProgress	別のバックアップの実行中は、新規バックアップを開始できません。	DRS は、別のバックアップで新規バックアップを開始できません。
DRFInternalProcessFailure	DRF 内部プロセスでエラーが発生しました。	DRS 内部プロセスでエラーしました。
DRFLA2MAFailure	DRF ローカル エージェントが、マスター エージェントに接続できません。	DRS ローカル エージェントがマスター エージェントに接続できません。
DRFLocalAgentStartFailure	DRF ローカル エージェントが開始されません。	DRS ローカル エージェントが開始されていない可能性があります。

アラーム名	説明	説明
DRFMA2LAFailure	DRF マスター エージェントがローカル エージェントに接続しません。	DRS マスター エージェントがローカル エージェントに接続
DRFMABackupComponentFailure	DRF は、少なくとも 1 つのコンポーネントをバックアップできません。	DRS は、コンポーネントをバックアップするよう
DRFMABackupNodeDisconnect	バックアップされるノードが、バックアップの完了前にマスターエージェントから切断されました。	DRS マスター エージェントが Unified Communications でバックアップ操作を
DRFMARestoreComponentFailure	DRF は、少なくとも 1 つのコンポーネントを復元できません。	DRS は、コンポーネントを復元するように要求しま
DRFMARestoreNodeDisconnect	復元されるノードが、復元の完了前にマスターエージェントから切断されました。	DRS マスター エージェントが Unified Communications で復元操作を実行して
DRFMasterAgentStartFailure	DRF マスター エージェントが開始されませんでした。	DRS マスター エージェントが実行している可能性があり
DRFNoRegisteredComponent	使用可能な登録済みコンポーネントがないため、バックアップが失敗しました。	使用可能な登録済みコンポーネントがないため、DRS バックアップ
DRFNoRegisteredFeature	バックアップする機能が選択されませんでした。	バックアップする機能を選択されませんでした。
DRFRestoreDeviceError	DRF 復元プロセスでデバイスへのアクセスに関する問題が発生しています。	DRS 復元プロセスは、デバイスにアクセスすることができませ
DRFRestoreFailure	DRF 復元プロセスが失敗しました。	DRS 復元プロセスでエラーが発生しました。
DRFSftpFailure	DRF SFTP 操作でエラーが発生しています。	DRS SFTP 操作でエラーが発生しています。

アラーム名	説明	説明
DRFSecurityViolation	DRF システムが、セキュリティ違反となる可能性がある悪意のあるパターンを検出しました。	DRF ネットワーク メッセージコードインジェクションやリトラバーサルなど、セキュリティ違反となる可能性がある悪意のあるパターンが含まれています。ワークメッセージがブロックされます。
DRFTruststoreMissing	ノードで IPsec 信頼ストアが見つかりません。	ノードで IPsec 信頼ストアが見つかりません。DRF ローカルエージェントが、マスターエージェントが見つかりません。
DRFUnknownClient	パブリッシャの DRF マスターエージェントが、クラスタ外部の不明なサーバからクライアント接続要求を受け取りました。要求は拒否されました。	パブリッシャの DRF マスターエージェントが、クラスタ外部の不明なサーバからクライアント接続要求を受け取りました。要求は拒否されました。
DRFBackupCompleted	DRF バックアップが正常に完了しました。	DRF バックアップが正常に完了しました。
DRFRestoreCompleted	DRF 復元が正常に完了しました。	DRF 復元が正常に完了しました。
DRFNoBackupTaken	現在のシステムの有効なバックアップが見つかりませんでした。	アップグレード/移行またはツール後に、現在のシステムにバックアップが見つかりませんでした。
DRFComponentRegistered	DRF により、要求されたコンポーネントが正常に登録されました。	DRF により、要求されたコンポーネントが正常に登録されました。
DRFRegistrationFailure	DRF 登録操作が失敗しました。	内部エラーが原因で、コンポーネントに対する DRF 登録操作が失敗しました。
DRFComponentDeRegistered	DRF は正常に要求されたコンポーネントの登録をキャンセルしました。	DRF は正常に要求されたコンポーネントの登録をキャンセルしました。
DRFDeRegistrationFailure	コンポーネントの DRF 登録解除リクエストが失敗しました。	コンポーネントの DRF 登録解除リクエストが失敗しました。
DRFFailure	DRF バックアップまたは復元プロセスが失敗しました。	DRF バックアップまたは復元プロセスでエラーが発生しました。
DRFRestoreInternalError	DRF 復元オペレーションでエラーが発生しました。復元は内部的にキャンセルされました。	DRF 復元オペレーションでエラーが発生しました。復元は内部的にキャンセルされました。

アラーム名	説明	説明
DRFLogDirAccessFailure	DRF は、ログディレクトリにアクセスできませんでした。	DRF は、ログディレクトリにアクセスできませんでした。
DRFDeRegisteredServer	DRF がサーバのすべてのコンポーネントを自動的に登録解除しました。	サーバが Unified Communication Manager クラスタから削除された可能性があります。
DRFSchedulerDisabled	設定された機能がバックアップで使用できないため、DRF スケジューラは無効になっています。	設定された機能がバックアップで使用できないため、DRF スケジューラは無効になっています。
DRFSchedulerUpdated	機能が登録解除されたため、DRF でスケジューラされたバックアップ設定が自動的に更新されます。	機能が登録解除されたため、DRF でスケジューラされたバックアップ設定が自動的に更新されます。

ライセンス予約

ライセンス予約



重要 次のライセンス機能テーブルは、Unified CM 14SU1 リリースまでサポートされています。

Unified Communication Manager を有効にした特定のライセンス予約またはパーマネントライセンス予約に対して復元操作を実行した後に、次の手順に従います。

表 91: ライセンス予約のディザスタリカバリシステム

復元後の状態	CSSM 上の製品	ソリューション
未登録	可	シスコに連絡して CSSM から製品を削除し、製品から登録してください。
	不可	何もする必要はありません

復元後の状態	CSSM 上の製品	ソリューション
予約を実行中です	可	次のいずれかの手順を実行します。 手順 1 : <ol style="list-style-type: none"> CSSM から製品の承認コードを取得します。 承認コード ライセンススマート予約の戻り値承認「<authorization-code>」を指定して、以下の CLI を実行します。 手順 2 : <ol style="list-style-type: none"> シスコに連絡して CSSM から製品を削除してください。
	いいえ	製品 ライセンススマート予約キャンセル から、CLI を実行します。
登録済み - 特定のライセンス予約または登録済み-ユニバーサルライセンス予約 (注) スマートエージェントは、ユニバーサルライセンス予約としてステータスを反映する場合がありますが、永久ライセンス予約機能用です。	可	<ol style="list-style-type: none"> 製品から以下の CLI ライセンススマート予約戻りを実行します。予約戻りコードがコンソールに出力されます。 製品を削除するには、CSSM で予約戻りコードを入力します。
	不可	製品 ライセンススマート予約戻り から、CLI を実行します。

ライセンス情報

ライセンス情報



Important 次のライセンス機能の表は、Unified CM 14SU2 リリース以降でサポートされています。

ライセンス情報を更新するために Unified Communication Manager を復元操作した後に、次の手順に従います。

Table 92: ライセンスのディザスタリカバリ システム

復元後の状態	バックアップの状態	CSSM またはサテライト上の製品	ソリューション
未登録	Unified Communication Manager を有効にした特定のライセンス予約またはパーマネントライセンス予約に対する復元操作	○	Cisco に連絡して CSSM から製品を削除し、Unified CM からライセンス予約を実行してください。
		なし	処置は不要です。
	CSSM またはサテライトに登録された Unified Communications Manager での復元操作	○	CSSM またはサテライトではアクションは必要ありません。 製品から再登録してください。
		なし	処置は不要です。
	CSSM に登録され、輸出制限付きライセンスが許可された Unified Communications Manager での復元操作	○	CSSM またはサテライトではアクションは必要ありません。 再登録し、製品から輸出制限ライセンスを申請してください。
		なし	処置は不要です。
	CSSM サテライトに登録され、輸出制限付きライセンスが許可された Unified Communications Manager での復元操作	○	CSSM および Cisco Smart Software Manager サテライトから製品を削除するには、シスコに連絡してください。 その後、製品から登録し、製品から輸出制限ライセンスを申請してください。
		なし	処置は不要です。

復元の連携動作と制約事項

復元の連携動作と制約事項

ディザスタリカバリシステムを使用して Cisco Unified Communications Manager または IM and Presence Service を復元する場合、以下の制約事項が適用されます。

Table 93: 復元の制約事項

制限事項	説明
エクスポートの制限	制限されたバージョンの DRS バックアップは、制限されたバージョンにのみ復元できます。また、制限されていないバージョンのバックアップは、制限されていないバージョンにのみ復元できます。Unified Communications Manager の米国輸出無制限バージョンにアップグレードした場合、その後、このソフトウェアの米国輸出制限バージョンへのアップグレード、または新規インストールを実行できなくなります。
プラットフォームの移行	ディザスタリカバリシステムを使用してプラットフォーム間で（たとえば、Windows から Linux へ、または Linux から Windows へ）データを移行することはできません。復元は、バックアップと同じ製品バージョンで実行する必要があります。Windows ベースのプラットフォームから Linux ベースのプラットフォームへのデータ移行については、『Data Migration Assistant User Guide』を参照してください。
HW の交換と移行	DRS 復元を実行してデータを新しいサーバに移行する場合、新しいサーバに古いサーバが使用していたのと同じ IP アドレスとホスト名を割り当てる必要があります。さらに、バックアップの取得時に DNS が設定されている場合、復元を実行する前に、同じ DNS 設定がある必要があります。 サーバの交換の詳細については、『Replacing a Single Server or Cluster for Cisco Unified Communications Manager』ガイドを参照してください。 また、ハードウェアの交換後は、証明書信頼リスト (CTL) クライアントを実行する必要もあります。後続ノード (サブスクリバ) サーバを復元しない場合には、CTL クライアントを実行する必要があります。他の場合、DRS は必要な証明書をバックアップします。詳細については、『Cisco Unified Communications Manager Security Guide』の「Installing the CTL Client」と「Configuring the CTL Client」の手順を参照してください。

制限事項	説明
クラスタ間のエクステンション モビリティ (Extension Mobility Cross Cluster)	バックアップ時にリモート クラスタにログインしていた Extension Mobility Cross Cluster ユーザは、復元後もログインしたままとなります。



Note Smart License Manager は、DRS バックアップ/復元の一部としてバックアップまたは復元されません。

Unified Communications Manager サーバーコンポーネントを正常に復元すると、Unified Communications Manager は未登録状態になります。その後、Unified Communications Manager を Cisco Smart Software Manager または Cisco Smart Software Manager サテライトに登録します。

バックアップを作成する前に製品がすでに登録されていたとしても、その製品を再登録してライセンス情報を更新する必要があります。

バックアップを取得する前に製品がすでに輸出制限付きライセンスの認可を受けており、製品インスタンスが Cisco Smart Software Manager または Cisco Smart Software Manager サテライトに存在する場合は、シスコに連絡して CSSM および Cisco Smart Software Manager サテライトから製品を削除し、サテライト展開を使用している間に製品から登録してください。直接導入する場合は、製品を再登録し、輸出制限ライセンスを申請してください。

Cisco Smart Software Manager または Cisco Smart Software Manager サテライトに製品を登録する方法の詳細については、ご使用のリリースの『[Cisco Unified Communications Manager システム設定ガイド](#)』を参照してください。

トラブルシューティング

より小さい仮想マシンへの DRS 復元の失敗

問題

IM and Presence サービス ノードをディスク容量がより小さい VM に復元すると、データベースの復元が失敗することがあります。

原因

大きいディスクサイズから小さいディスクサイズに移行したときに、この障害が発生します。

解決策

2 個の仮想ディスクがある OVA テンプレートから、復元用の VM を展開します。



第 **IX** 部

トラブルシューティング

- [トラブルシューティングの概要](#) (527 ページ)
- [トラブルシューティング ツール](#) (531 ページ)
- [TAC とのケースのオープン](#) (563 ページ)



第 36 章

トラブルシューティングの概要

ここでは、Unified Communications Manager のトラブルシューティングに必要な背景情報と使用できるリソースについて説明します。

- [Cisco Unified Serviceability](#) (527 ページ)
- [Cisco Unified Communications Operating System Administration](#) (528 ページ)
- 一般的な問題解決モデル (528 ページ)
- ネットワーク障害への事前準備 (529 ページ)
- 詳細情報の入手先 (530 ページ)

Cisco Unified Serviceability

Cisco Unified Serviceability は Unified Communications Manager 用の Web ベースのトラブルシューティングツールです。このツールには、管理者がシステム問題をトラブルシューティングできるように次の機能が備えられています。

- トラブルシューティング用に Unified Communications Manager サービスのアラームとイベントを保存し、アラーム メッセージの定義を提供します。
- トラブルシューティング用に Unified Communications Manager サービスのトレース情報をさまざまなログファイルに保存します。管理者はトレース情報の設定、収集、および表示を行うことができます。
- Real-Time Monitoring Tool (RTMT) を使用して、Unified Communications Manager クラスターのコンポーネントの動作をリアルタイムで監視します。
- Unified Communications Manager CDR Analysis and Reporting (CAR) を使用して、Quality of Service、トラフィック、課金情報についてのレポートを生成します。
- [サービスの開始 (Service Activation)] ウィンドウによりアクティブ化、非アクティブ化、および表示を行うことができる機能サービスを提供する。
- 機能とネットワークサービスを開始および停止するためのインターフェイスを提供する。
- Cisco Unified Serviceability のツールに関連付けられているレポートをアーカイブします。

- Unified Communications Managerが、SNMPのリモート管理とトラブルシューティングのために管理対象デバイスとして動作できるようにする。
- 1つのサーバ（またはクラスタ内のすべてのサーバ）のログパーティションのディスク使用を監視します。

[ナビゲーション (Navigation)] ドロップダウンリストボックスから [Cisco Unified Serviceability] を選択して、[Cisco Unified Communications Manager Administration] ウィンドウから Cisco Unified Serviceability にアクセスします。 Unified Communications Manager ソフトウェアをインストールすると Cisco Unified Serviceability が自動的にインストールされ、使用可能になります。

サービスアビリティツールの詳細と手順については、『*Cisco Unified Serviceability Administration Guide*』を参照してください。

Cisco Unified Communications Operating System Administration

Cisco Unified Communications Operating System Administration を使用すると、次のタスクを実行して *Cisco Unified Communications Operating System* を設定および管理できます。

- ソフトウェアとハードウェアのステータスを確認する。
- IP アドレスの確認と更新を行う。
- 他のネットワーク デバイスに ping を送信する。
- Network Time Protocol サーバの管理
- システム ソフトウェアおよびオプションをアップグレードする。
- システムを再起動します。

サービスアビリティツールの詳細と設定手順については、[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。

一般的な問題解決モデル

テレフォニーまたは IP ネットワーク環境のトラブルシューティングを行う場合は、症状を定義し、その症状の原因と考えられるすべての問題を特定し、考えられる各問題を、症状がなくなるまで可能性の高い順に体系的に取り除いていきます。

次の手順は、問題解決プロセスで使用するガイドラインを示しています。

手順

1. ネットワークの問題を分析し、問題を明確に記述します。症状と潜在的な原因を定義します。
2. 潜在的な原因を特定するための事実を収集します。

3. 収集した事実を元に、潜在的な原因を検証します。
4. それらの原因に基づいて処置プランを作成します。最も起こりうる問題から始めて、1つの変数だけを操作する計画を考えます。
5. 処置プランを実施し、テストして症状が消えるかどうかを確認しながら、各手順を慎重に実行します。
6. 結果を分析し、問題が解決したかどうかを確認します。問題が解決している場合は、プロセスは完了です。
7. 問題が解決していない場合は、リストで次に可能性の高い原因に基づいて処置プランを作成します。4 (529 ページ) に戻り、問題が解決するまでプロセスを繰り返します。

処置プランの実施中に行った変更は、必ず元に戻してください。変数は一度に1つだけ変更します。



(注) 一般的な原因と処置（このマニュアルで概要を説明しているもの、または環境に応じて特定したもの）をすべて実施しても問題が解決しない場合は、Cisco TAC にお問い合わせください。

ネットワーク障害への事前準備

ネットワーク障害からの回復は、事前準備をしておくことで容易に行うことができます。次の質問に答え、ネットワーク障害への事前準備ができているかどうかを確認します。

- ネットワーク上のすべてのデバイスの物理的な場所とそれらの接続方法の概要を示した、相互接続されたネットワークの正確な物理および論理マップがありますか。また、ネットワークアドレス、ネットワーク番号、サブネットワークを記述した論理マップがありますか。
- ネットワークに実装されているすべてのネットワークプロトコルのリスト、各プロトコルに関連付けられているネットワーク番号、サブネットワーク、ゾーン、およびエリアの正確なリストがありますか。
- どのプロトコルがルーティングされているか、および各プロトコルについての正確かつ最新の設定情報を把握していますか。
- どのプロトコルがブリッジングされているかを把握していますか。それらのブリッジに設定されているフィルタがありますか。また、その設定のコピーはありますか。そのコピーは Unified Communications Manager に適用できますか。
- インターネットへの接続も含め、外部ネットワークへのすべての接点を把握しているか。各外部ネットワーク接続について、使用されているルーティングプロトコルを知っていますか。
- 現在の問題とベースラインを比較できるように、通常のネットワーク動作とパフォーマンスについて組織で文書化していますか。

これらの質問に「はい」と答えることができれば、障害から迅速に回復できます。

詳細情報の入手先

さまざまな IP テレフォニー トピックに関する情報については、次のリンクを使用してください。

- 関連する Cisco IP テレフォニー アプリケーションおよび製品に関する詳細については、『*Cisco Unified Communications Manager Documentation Guide*』を参照してください。次の URL は、マニュアルへのパスの例です。

https://www.cisco.com/en/US/products/sw/voicesw/ps556/products_documentation_roadmaps_list.html

- Cisco Unity に関連するマニュアルについては、次の URL を参照してください。
https://www.cisco.com/en/US/products/sw/voicesw/ps2237/tsd_products_support_series_home.html
- Cisco Emergency Responder に関連するマニュアルについては、次の URL を参照してください。
https://www.cisco.com/en/US/products/sw/voicesw/ps842/tsd_products_support_series_home.html
- Cisco Unified IP Phone に関連するマニュアルについては、次の URL を参照してください。
https://www.cisco.com/en/US/products/hw/phones/ps379/tsd_products_support_series_home.html
- IP テレフォニー ネットワークの設計とトラブルシューティングについては、www.cisco.com/go/srndにある『Cisco IP Telephony Solution Reference Network Design Guides』を参照してください。



第 37 章

トラブルシューティング ツール

ここでは、Unified Communications Manager の設定、監視、およびトラブルシューティングを行うために使用するツールやユーティリティについて説明し、テストの繰り返しや同一データの再収集を回避するためのデータ収集に関する一般的なガイドラインを提供します。



(注) このマニュアルにリストされている URL サイトの一部にアクセスするには、登録ユーザとしてログインする必要があります。

- [Cisco Unified サービスアビリティ トラブルシューティング ツール \(531 ページ\)](#)
- [コマンドラインインターフェイス \(533 ページ\)](#)
- [Kerneldump ユーティリティ \(533 ページ\)](#)
- [ネットワーク管理 \(536 ページ\)](#)
- [スニファトレース \(538 ページ\)](#)
- [デバッグ \(538 ページ\)](#)
- [Cisco Secure Telnet \(539 ページ\)](#)
- [パケットキャプチャ \(539 ページ\)](#)
- [一般的なトラブルシューティングのタスク、ツール、およびコマンド \(547 ページ\)](#)
- [トラブルシューティングのヒント \(550 ページ\)](#)
- [システム履歴ログ \(552 ページ\)](#)
- [監査ロギング \(555 ページ\)](#)
- [Cisco Unified Communications Manager サービスが稼働しているかどうかの確認 \(560 ページ\)](#)

Cisco Unified サービスアビリティ トラブルシューティング ツール

さまざまな Unified Communications Manager システムを監視および分析するために、Cisco Unified Serviceability が提供する次のさまざまなタイプのツールの詳細については、『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。

表 94: Serviceability ツール

用語	定義
Cisco Unified Real-Time Monitoring Tool (RTMT)	<p>このツールは、Unified Communications Manager のデバイスとパフォーマンス カウンタに関するリアルタイムな情報を提供するとともに、トレースの収集を可能にします。</p> <p>パフォーマンス カウンタは、システム固有か、または Unified Communications Manager 固有である場合があります。オブジェクトは、Cisco Unified IP Phone や Unified Communications Manager などの、特定のデバイスまたは機能に対する同等のカウンタの論理的なグループで構成されています。カウンタによって、システム パフォーマンスのさまざまな側面が測定されます。登録済み電話機の数、試行されたコール数、進行中のコール数などの統計が測定されます。</p>
アラーム	<p>管理者は、アラームを使用して、Unified Communications Manager システムの実行時のステータスや状態情報を取得します。アラームには、説明や推奨処置など、システムの問題に関する情報が含まれています。</p> <p>管理者は、アラーム定義データベースでアラーム情報を検索します。アラーム定義には、アラームの説明と推奨処置が含まれています。</p>
Trace	<p>管理者とシスコのエンジニアは、トレースファイルを使用して Unified Communications Manager サービスの問題に関する特定の情報を取得し、Cisco Unified Serviceability 設定されたトレース情報をトレース ログ ファイルに送信します。トレース ログ ファイルには、SDI と SDL の 2 種類があります。</p> <p>各サービスには、デフォルトのトレース ログが含まれています。システムによって、サービスからのシステム診断インターフェイス (SDI) 情報がトレースされ、実行時のイベントとトレースがログ ファイルに記録されます。</p> <p>SDL トレース ログ ファイルには、Cisco CallManager や Cisco CTIManager などのサービスからのコール処理情報が含まれています。システムによって、コールの信号配信レイヤ (SDL) がトレースされ、状態遷移がログ ファイルに記録されます。</p> <p>(注) 通常は、Cisco Technical Assistance Center (TAC) の指示に従って、SDL トレースだけを収集することになります。</p>
Quality Report Tool	<p>この用語は、Cisco Unified Serviceability の音声品質と一般的な問題をレポートするユーティリティを示しています。</p>

用語	定義
Serviceability Connector	Cisco Webex Serviceability サービスにより、シスコのテクニカル アシスタンス スタッフがインフラストラクチャに関する問題を診断できる速度が向上します。診断ログと情報を検索し、取得して、SR ケースに保存するタスクを自動化します。このサービスは、診断シグニチャに対する分析もトリガーするため、TAC はオンプレミス機器の問題をより効率的に識別して解決できます。

コマンドラインインターフェイス

コマンドラインインターフェイス (CLI) を使用すると、Unified Communications Manager システムにアクセスし、基本的なメンテナンスや障害からの回復を行うことができます。ハードワイヤされた端末 (システム モニタとキーボード) を使用するか、または SSH セッションを実行することによってシステムにアクセスします。

インストール時に、アカウント名とパスワードが作成されます。パスワードはインストール後に変更できますが、アカウント名は変更できません。

コマンドとは、システムに特定の機能を実行させるテキスト命令を表します。コマンドは、単独で使用される場合と、必須または任意の引数を伴う場合があります。

レベルは、コマンドの集合で構成されます。たとえば、show はレベルを示し、show status はコマンドを示します。また、各レベルとコマンドには、特権レベルが関連付けられています。ユーザは、適切な特権レベルを持っている場合にだけ、コマンドを実行できます。

Unified Communications Manager の CLI コマンドセットの詳細については、『Cisco Unified 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』を参照してください。

Kerneldump ユーティリティ

Kerneldump ユーティリティにより、セカンダリ サーバを要求することなしに、該当するマシンでクラッシュ ダンプ ログをローカルに収集できます。

Unified Communications Manager クラスタでは、Kerneldump ユーティリティがサーバで有効であることを確認するだけで、クラッシュ ダンプ情報を収集できます。



- (注) シスコでは、より効果的なトラブルシューティングを実現するため、Unified Communications Manager のインストール後に、Kerneldump ユーティリティが有効であることを確認するよう推奨しています。Kerneldump ユーティリティの設定をまだ行っていない場合は、Unified Communications Manager をサポート対象のアプライアンスリリースからアップグレードする前に行ってください。



重要 Kerneldump ユーティリティをイネーブル化またはディセーブル化を行うには、ノードのリポートが必要です。リポートが許容されるウィンドウ以外では、**enable** コマンドを実行しないでください。

Cisco Unified Communications オペレーティング システムのコマンドライン インターフェイス (CLI) を使用すると、Kerneldump ユーティリティのイネーブル化、ディセーブル化、ステータス確認を実行できます。

次の手順を利用して Kerneldump ユーティリティをイネーブル化します。

ユーティリティによって収集されるファイルの処理

Kerneldump ユーティリティから送信されたクラッシュ情報を表示するには、*Cisco Unified Real-Time Monitoring Tool* またはコマンドライン インターフェイス (CLI) を使用します。*Cisco Unified Real-Time Monitoring Tool* を使用して netdump ログを収集するには、[トレースおよびログ セントラル (Trace & Log Central)] の [ファイルの収集 (Collect Files)] オプションを選択します。[システム サービス/アプリケーションの選択 (Select System Services/Applications)] タブで、[Kerneldump ログ (Kerneldump logs)] チェックボックスをオンにします。*Cisco Unified Real-Time Monitoring Tool* を使用したファイルの収集の詳細については、『*Cisco Unified Real-Time Monitoring Tool Administration Guide*』を参照してください。

CLI を使用して kerneldump ログを収集するには、クラッシュ ディレクトリのファイルに対して「file」 CLI コマンドを使用します。これらは「activelog」のパーティションの下にあります。ログ ファイル名は、kerneldump クライアントの IP アドレスで始まり、ファイルが作成された日付で終わります。ファイル コマンドの詳細については、『*Command Line Interface Reference Guide for Cisco Unified Solutions*』を参照してください。

Kerneldump ユーティリティの有効化

次の手順を利用して Kerneldump ユーティリティをイネーブル化します。カーネル クラッシュが発生した場合、ユーティリティは、クラッシュの収集とダンプのメカニズムを提供します。ローカル サーバまたは外部サーバにログをダンプするユーティリティを設定できます。

手順

ステップ 1 コマンドライン インターフェイスにログインします。

ステップ 2 次のいずれかを実行します。

- ローカル サーバ上のカーネル クラッシュをダンプするには、`utils os kernelcrash enable` CLI コマンドを実行します。
- 外部サーバにカーネル クラッシュをダンプするには、外部サーバの IP アドレスを指定して `utils os kerneldump ssh enable <ip_address>` CLI コマンドを実行します。

ステップ 3 サーバをリブートします。

例



- (注) kerneldump ユーティリティを無効にする必要がある場合、`utils os kernelcrash disable` CLI コマンドを実行してローカルサーバのコア ダンプを無効にし、`utils os kerneldump ssh disable <ip_address>` CLI コマンドを実行して外部サーバ上のユーティリティを無効にします。

次のタスク

コア ダンプの指示に従ってリアルタイム モニタリング ツールで電子メールアラートを設定します。詳細については、[コア ダンプの電子メールアラートの有効化 \(326 ページ\)](#) を参照してください。

kerneldump ユーティリティおよびトラブルシューティングについては、『*Troubleshooting Guide for Cisco Unified Communications Manager*』を参照してください。

コア ダンプの電子メール アラートの有効化

コア ダンプが発生するたびに管理者に電子メールを送信するようにリアルタイム モニタリング ツールを設定するには、次の手順を使用します。

手順

- ステップ 1** [システム (System)] > [ツール (Tools)] > [アラート セントラル) Alert Central)] の順に選択します。
- ステップ 2** [CoreDumpFileFound] アラートを右クリックし、[アラート/プロパティの設定 (Set Alert/Properties)] を選択します。
- ステップ 3** ウィザードの指示に従って優先条件を設定します。
- [アラート プロパティ: 電子メール通知 (Alert Properties: Email Notification)] ポップアップで、[電子メールの有効化 (Enable Email)] がオンになっていることを確認し、[設定 (Configure)] をクリックしてデフォルトのアラート アクションを設定します。これにより管理者に電子メールが送信されます。
 - プロンプトに従って、受信者電子メールアドレスを [追加 (Add)] します。このアラートがトリガーされると、デフォルトのアクションは、このアドレスへの電子メールの送信になります。
 - [保存 (Save)] をクリックします。
- ステップ 4** デフォルトの電子メール サーバを設定します。

- a) [システム (System)] > [ツール (Tools)] > [アラート (Alert)] > [電子メール サーバの設定 (Config Email Server)] の順に選択します。
- b) 電子メールアラートを送信する電子メールサーバーとポート情報を入力します。
- c) (オプション) SMTP サーバーへの暗号化された通信チャネルを有効にするには、[TLS モードの有効化 (Enable TLS mode)] チェックボックスをオンにします。
- d) (オプション) 受信者の電子メールアドレスの認証を要求するには、[認証モードの有効化 (Enable Authentication mode)] チェックボックスをオンにします。

(注) [ユーザー名 (Username)] および [パスワード (Password)] フィールドにアクセスできるのは、[認証モードの有効化 (Enable Authentication mode)] チェックボックスが有効になっている場合のみです。

- e) [Username] フィールドにユーザー名を入力します。
- f) パスワードを [Password] フィールドに入力します。
- g) [送信するユーザー ID (Send User ID)] を入力します。
- h) [OK] をクリックします。

ネットワーク管理

Unified Communications Manager のリモート有用性には、ネットワーク管理ツールを使用します。

- システム ログ管理
- Cisco Discovery Protocol のサポート
- 簡易ネットワーク管理プロトコル (SNMP) のサポート

これらのネットワーク管理ツールの詳細については、それぞれの項に記載された URL にあるマニュアルを参照してください。

システム ログ管理

Resource Manager Essentials (RME) にパッケージされている Cisco Syslog Analysis は、他のネットワーク管理システムにも適応可能ですが、シスコ デバイスから送信される Syslog メッセージの管理に最適な方法を提供します。

Cisco Syslog Analyzer は、複数アプリケーションのシステム ログの共通ストレージを提供し、その分析を行う Cisco Syslog Analysis のコンポーネントとして機能します。もう 1 つの主要コンポーネントである Syslog Analyzer Collector は、Unified Communications Manager サーバからログメッセージを収集します。

これら 2 つの Cisco アプリケーションが連動し、Cisco Unified Communication ソリューションの集中型システム ログ サービスを提供します。

RMEのマニュアルについては、
http://www.cisco.com/en/US/products/sw/cscowork/ps2073/products_tech_note09186a00800a7275.shtml
を参照してください。

Cisco Discovery Protocol のサポート

Cisco Discovery Protocol がサポートされているため、Unified Communications Manager サーバの検出および管理が可能です。

RMEのマニュアルについては、
http://www.cisco.com/en/US/products/sw/cscowork/ps2073/products_tech_note09186a00800a7275.shtml
を参照してください。

簡易ネットワーク管理プロトコル (SNMP) のサポート

ネットワーク管理システム (NMS) では、業界標準インターフェイスである SNMP を使用して、ネットワーク デバイス間で管理情報が交換されます。TCP/IP プロトコルスイートの一部である SNMP を使用すると、管理者はリモートでネットワークのパフォーマンスを管理し、ネットワークの問題を検出および解決し、ネットワークの拡張計画を立てることができます。

SNMP管理のネットワークは、管理対象デバイス、エージェント、およびネットワーク管理システムという3つの主要コンポーネントで構成されています。

- 管理対象デバイスは、SNMP エージェントを含み、管理対象ネットワークに存在するネットワーク ノードを指します。管理対象デバイスには管理情報が収集および格納され、その情報は SNMP を使用することによって利用可能になります。
- エージェントは、ネットワーク管理ソフトウェアとして、管理対象デバイスに存在します。エージェントには、管理情報のローカルな知識が蓄積され、SNMP と互換性のある形式に変換されます。
- ネットワーク管理システムは、SNMP 管理アプリケーションと、そのアプリケーションが実行されるコンピュータで構成されています。NMS では、管理対象デバイスをモニタおよび制御するアプリケーションが実行されます。ネットワーク管理に必要な処理とメモリリソースの大部分は、NMS によって提供されます。次の NMS は Unified Communications Manager と互換性を持っています。
 - CiscoWorks Common Services Software
 - HP OpenView
 - SNMP および Unified Communications Manager SNMP インターフェイスをサポートしているサードパーティ製アプリケーション

スニファトレース

通常、スニファトレースは、VLANまたは問題の情報が含まれるポート（CatOS、Cat6K-IOS、XL-IOS）にまたがるように設定された Catalyst ポートに、ラップトップやその他のスニファタ搭載デバイスを接続することによって収集します。利用可能なポートが空いていない場合は、スニファタ搭載デバイスを、スイッチとデバイスの上に挿入されるハブに接続します。



ヒント TAC のエンジニアがトレースを読解しやすいように、TAC で広く使用されている Sniffer Pro ソフトウェアを使用することを推奨します。

IP Phone、ゲートウェイ、Unified Communications Manager など、関連するすべての装置の IP/MAC アドレスを利用可能にしておいてください。

デバッグ

debug 特権 EXEC コマンドの出力は、プロトコルのステータスおよびネットワーク アクティビティ全般に関する、さまざまなネットワーク間イベントについての診断情報を提供します。

端末エミュレータソフトウェア（ハイパーターミナルなど）を設定し、デバッグ出力をファイルに取得できるようにしてください。ハイパーターミナルで、[転送 (Transfer)] をクリックし、[テキストのキャプチャ (Capture Text)] をクリックして、適切なオプションを選択します。

IOS 音声ゲートウェイデバッグを実行する前に、**servicetimestampsdebugdatetimemsec** がゲートウェイでグローバルに設定されていることを確認してください。



(注) 運用時間中にライブ環境でデバッグを収集することは避けてください。

運用時間外にデバッグを収集することを推奨します。ライブ環境でデバッグを収集する必要がある場合は、**no logging console oyloggingbuffered** を設定します。デバッグを収集するには、**show log** を使用します。

デバッグは長くなることがあるため、コンソールポート（デフォルトの **logging console**）またはバッファ (**logging buffer**) でデバッグを直接収集します。セッションを介してデバッグを収集すると、デバイスのパフォーマンスが低下して、デバッグが不完全となり、デバッグを再収集する必要が生じることがあります。

デバッグを停止するには、**no debug all** コマンドまたは **undebug all** コマンドを使用します。**show debug** コマンドを使用して、デバッグがオフになっていることを確認してください。

Cisco Secure Telnet

シスコ サービス エンジニア (CSE) は、*Cisco Secure Telnet* を使用して、サイト上の Unified Communications Manager ノードに対して透過的にファイアウォールアクセスを実行できます。*Cisco Secure Telnet* は、強力な暗号化を使用して、シスコ内の特別な Telnet クライアントを、ファイアウォールの内側にある Telnet デーモンに接続できます。このセキュアな接続により、ファイアウォールを変更せずに、Unified Communications Manager ノードの監視およびトラブルシューティングをリモートで行うことができます。



(注) シスコは、お客様の承諾を得た場合にだけこのサービスを提供します。サイトに、このプロセスの開始を支援するネットワーク管理者を配置する必要があります。

パケット キャプチャ

ここでは、パケット キャプチャについて説明します。

関連トピック

- [パケット キャプチャの概要 \(539 ページ\)](#)
- [パケット キャプチャの設定チェックリスト \(540 ページ\)](#)
- [Standard Packet Sniffer Users アクセス コントロールグループへのエンドユーザの追加 \(541 ページ\)](#)
- [パケット キャプチャのサービス パラメータの設定 \(541 ページ\)](#)
- [\[電話の設定 \(Phone Configuration\)\] ウィンドウでのパケット キャプチャの設定 \(542 ページ\)](#)
- [\[ゲートウェイの設定 \(Gateway Configuration\)\] ウィンドウおよび\[トランクの設定 \(Trunk Configuration\)\] ウィンドウでのパケット キャプチャの設定 \(543 ページ\)](#)
- [パケット キャプチャの設定値 \(545 ページ\)](#)
- [キャプチャしたパケットの分析 \(547 ページ\)](#)

パケット キャプチャの概要

メディアや TCP パケットをスニフィングするサードパーティ製トラブルシューティング ツールは、暗号化をイネーブルにしたあとは機能しません。このため、問題が発生した場合は、Unified Communications Manager を使用して次のタスクを行う必要があります。

- Unified Communications Manager とデバイスとの間で交換されるメッセージのパケットの分析 (Cisco Unified IP Phone [SIP と SCCP]、Cisco IOS MGCP ゲートウェイ、H.323 ゲートウェイ、H.323/H.245/H.225 トランク、または SIP トランク)。
- デバイス間の Secure Real Time Protocol (SRTP) パケットのキャプチャ。

- メッセージからのメディア暗号キー情報の抽出、およびデバイス間のメディアの復号化。



ヒント このタスクを複数のデバイスに対して同時に実行すると、CPU使用率が高くなり、コール処理が中断される可能性があります。このタスクは、コール処理が中断される危険性が最も少ないときに実行することを強く推奨します。

詳細については、[Cisco Unified Communications Manager セキュリティ ガイド](#)を参照してください。

パケット キャプチャの設定チェックリスト

必要なデータを抽出し、分析するには、次の作業を実行します。

手順

1. エンドユーザを Standard Packet Sniffer Users グループに追加します。
2. Cisco Unified Communications Manager Administrationの [サービス パラメータ設定 (Service Parameter Configuration)] ウィンドウで、パケット キャプチャのサービス パラメータを設定します。たとえば、Packet Capture Enable サービス パラメータを設定します。
3. [電話の設定 (Phone Configuration)]、[ゲートウェイの設定 (Gateway Configuration)]、または [トランクの設定 (Trunk Configuration)] の各ウィンドウで、デバイスごとのパケット キャプチャの設定を行います。



(注) パケット キャプチャは、複数のデバイスで同時にはイネーブルにしないことを強く推奨します。このタスクによって、ネットワークで使用されている CPU の使用率が上昇する可能性があるためです。

4. 該当するデバイス間でスニファトレースを使用して、SRTPパケットをキャプチャします。使用しているスニファトレースツールに対応したマニュアルを参照してください。
5. パケットをキャプチャしたら、Packet Capture Enable サービス パラメータを False に設定します。
6. パケットの分析に必要なファイルを収集します。
7. Cisco Technical Assistance Center (TAC) がパケットを分析します。このタスクについては、TAC に直接お問い合わせください。

関連トピック

[Standard Packet Sniffer Users アクセスコントロールグループへのエンドユーザの追加](#) (541 ページ)

[キャプチャしたパケットの分析](#) (547 ページ)

[\[ゲートウェイの設定 \(Gateway Configuration\) \]ウィンドウおよび\[トランクの設定 \(Trunk Configuration\) \]ウィンドウでのパケットキャプチャの設定 \(543 ページ\)](#)

[\[電話の設定 \(Phone Configuration\) \]ウィンドウでのパケットキャプチャの設定 \(542 ページ\)](#)

[パケットキャプチャのサービスパラメータの設定 \(541 ページ\)](#)

[パケットキャプチャの設定値 \(545 ページ\)](#)

Standard Packet Sniffer Users アクセスコントロールグループへのエンドユーザの追加

Standard Packet Sniffer Users グループに所属するユーザは、パケットキャプチャをサポートしているデバイスについて、パケットキャプチャモードとパケットキャプチャ時間を設定できます。ユーザが Standard Packet Sniffer Users アクセスコントロールグループに含まれていない場合、そのユーザはパケットキャプチャを開始できません。

次の手順では、エンドユーザを Standard Packet Sniffer アクセス制御グループに追加する方法について説明します。この手順では、[Cisco Unified Communications Manager アドミニストレーションガイド](#)の説明に従って、Cisco Unified Communications Manager Administrationでエンドユーザを設定したことを前提としています。

手順

1. [Cisco Unified Communications Manager アドミニストレーションガイド](#)の説明に従って、アクセス制御グループを検索します。
2. [検索/リスト (Find/List)]ウィンドウが表示されたら、[標準パケットスニファユーザ (Standard Packet Sniffer Users)]リンクをクリックします。
3. [グループにユーザを追加 (Add Users to Group)]ボタンをクリックします。
4. [Cisco Unified Communications Manager アドミニストレーションガイド](#)の説明に従って、エンドユーザを追加します。
5. ユーザを追加したら、[保存 (Save)]をクリックします。

パケットキャプチャのサービスパラメータの設定

パケットキャプチャのパラメータを設定するには、次の手順を実行します。

手順

1. Unified Communications Managerで、[システム (System)]> [サービスパラメータ (Service Parameters)]を選択します。
2. [サーバ (Server)]ドロップダウンリストボックスで、Cisco CallManager サービスをアクティブにした Active サーバを選択します。

3. [サービス (Service)] ドロップダウンリストボックスで、[Cisco CallManager (アクティブ) (Cisco CallManager (Active))] サービスを選択します。
4. [TLS パケット キャプチャ設定 (TLS Packet Capturing Configuration)] ペインまでスクロールして、パケット キャプチャを設定します。



ヒント サービスパラメータについては、ウィンドウに表示されているパラメータ名または疑問符をクリックしてください。



(注) パケットキャプチャを実行するには、Packet Capture Enable サービスパラメータを True に設定する必要があります。

5. 変更内容を有効にするには、[保存 (Save)] をクリックします。
6. パケットキャプチャの設定を続行できます。

関連トピック

[\[ゲートウェイの設定 \(Gateway Configuration\) \]ウィンドウおよび\[トランクの設定 \(Trunk Configuration\) \]ウィンドウでのパケットキャプチャの設定 \(543 ページ\)](#)

[\[電話の設定 \(Phone Configuration\) \]ウィンドウでのパケットキャプチャの設定 \(542 ページ\)](#)

[電話の設定 (Phone Configuration)]ウィンドウでのパケットキャプチャの設定

[サービスパラメータ (Service Parameter)]ウィンドウでパケットキャプチャをイネーブルにしたら、Cisco Unified Communications Manager Administrationの [電話の設定 (Phone Configuration)]ウィンドウで、デバイスごとにパケットキャプチャを設定できます。

電話機ごとに、パケットキャプチャをイネーブルまたはディセーブルにします。パケットキャプチャのデフォルト設定は、None です。



注意 パケットキャプチャは、複数の電話機で同時にはイネーブルにしないことを強く推奨します。このタスクによって、ネットワークで使用されている CPU の使用率が上昇する可能性があるためです。

パケットをキャプチャしない場合、またはタスクを完了した場合は、Packet Capture Enable サービスパラメータを False に設定します。

電話機のパケットキャプチャを設定するには、次の手順を実行します。

手順

1. パケット キャプチャを設定する前に、パケット キャプチャの設定に関するトピックを参照してください。
2. [Cisco Unified Communications Manager システム設定ガイド](#)の説明に従って、SIP 電話機または SCCP 電話機を検索します。
3. [電話の設定 (Phone Configuration)]ウィンドウが表示されたら、「[パケット キャプチャの設定値](#)」の説明に従って、トラブルシューティングの設定を行います。
4. 設定が完了したら、[保存 (Save)]をクリックします。
5. [リセット (Reset)]ダイアログボックスで、[OK] をクリックします。



ヒント Cisco Unified Communications Manager Administrationからデバイスをリセットするように求められますが、パケットをキャプチャするためにデバイスをリセットする必要はありません。

この他の手順

該当するデバイス間でスニファトレースを使用して、SRTP パケットをキャプチャします。

パケットをキャプチャしたら、Packet Capture Enable サービス パラメータを False に設定します。

関連トピック

[キャプチャしたパケットの分析](#) (547 ページ)

[パケット キャプチャの設定チェックリスト](#) (540 ページ)

[ゲートウェイの設定 (Gateway Configuration)]ウィンドウおよび[トランクの設定 (Trunk Configuration)]ウィンドウでのパケットキャプチャの設定

次のゲートウェイおよびトランクは、Unified Communications Managerでのパケットキャプチャをサポートしています。

- Cisco IOS MGCP ゲートウェイ
- H.323 ゲートウェイ
- H.323/H.245/H.225 トランク
- SIP トランク



ヒント パケットキャプチャは、複数のデバイスで同時にはイネーブルにしないことを強く推奨します。このタスクによって、ネットワークで使用されている CPU の使用率が上昇する可能性があるためです。

パケットをキャプチャしない場合、またはタスクを完了した場合は、**Packet Capture Enable** サービスパラメータを **False** に設定します。

[ゲートウェイの設定 (Gateway Configuration)] ウィンドウまたは [トランクの設定 (Trunk Configuration)] ウィンドウでパケットキャプチャの設定を行うには、次の手順を実行します。

手順

1. パケットキャプチャを設定する前に、パケットキャプチャの設定に関するトピックを参照してください。
2. 次のいずれかの操作を行います。
 - [Cisco Unified Communications Manager システム設定ガイド](#)の説明に従って、Cisco IOS MGCP ゲートウェイを検索します。
 - [Cisco Unified Communications Manager システム設定ガイド](#)の説明に従って、H.323 ゲートウェイを検索します。
 - [Cisco Unified Communications Manager システム設定ガイド](#)の説明に従って、H.323、H.245、または H.225 トランクを検索します。
 - [Cisco Unified Communications Manager システム設定ガイド](#)の説明に従って、SIP トランクを検索します。
3. 設定ウィンドウが表示されたら、[パケットキャプチャモード (Packet Capture Mode)] と [パケットキャプチャ時間 (Packet Capture Duration)] の設定値を確認します。



ヒント Cisco IOS MGCP ゲートウェイを見つけたら、Cisco IOS MGCP ゲートウェイ用のポートを [Cisco Unified Communications Manager アドミニストレーションガイド](#)の説明に従って設定してあることを確認します。Cisco IOS MGCP ゲートウェイのパケットキャプチャ設定値は、エンドポイント識別子の [ゲートウェイの設定 (Gateway Configuration)] ウィンドウに表示されます。このウィンドウにアクセスするには、音声インターフェイスカードのエンドポイント識別子をクリックします。

4. 「[パケットキャプチャの設定値](#)」の説明に従って、トラブルシューティングを設定します。
5. パケットキャプチャを設定したら、[保存 (Save)] をクリックします。
6. [リセット (Reset)] ダイアログボックスで、[OK] をクリックします。



ヒント Cisco Unified Communications Manager Administrationからデバイスをリセットするように求められますが、パケットをキャプチャするためにデバイスをリセットする必要はありません。

この他の手順

該当するデバイス間でスニファトレースを使用して、SRTP パケットをキャプチャします。

パケットをキャプチャしたら、Packet Capture Enable サービス パラメータを False に設定します。

関連トピック

[キャプチャしたパケットの分析](#) (547 ページ)

[パケットキャプチャの設定チェックリスト](#) (540 ページ)

パケットキャプチャの設定値

次の表に、ゲートウェイ、トランク、および電話機にパケットキャプチャを設定する際の [パケットキャプチャモード (Packet Capture Mode)] 設定と [パケットキャプチャ時間 (Packet Capture Duration)] 設定について説明します。

設定	説明
<p>[パケットキャプチャモード (Packet Capture Mode)]</p>	<p>この設定値は、暗号化のトラブルシューティングを行う場合にだけ使用します。パケットキャプチャを実行すると、CPUの使用率が上昇して、コール処理が妨げられる可能性があります。ドロップダウンリストボックスで、次のいずれかのオプションを選択します。</p> <ul style="list-style-type: none"> • [なし (None)]: このオプションは、パケットキャプチャが発生しないことを示します (デフォルト設定)。パケットキャプチャが完了すると、Unified Communications Managerは[パケットキャプチャモード (Packet Capture Mode)]を[なし (None)]に設定します。 • バッチ処理モード (Batch Processing Mode) : Unified Communications Manager復号化された (または暗号化されていない) メッセージをファイルに書き込み、システムが各ファイルを暗号化します。毎日、システムは新しい暗号化キーを使用して新しいファイルを作成します。ファイルを7日間保存する Unified Communications Manager は、ファイルを暗号化するキーも安全な場所に保存します。Unified Communications Manager は、ファイルを PktCap 仮想ディレクトリに保存します。1つのファイルの中に、タイムスタンプ、送信元 IP アドレス、送信元 IP ポート、宛先 IP アドレス、パケットのプロトコル、メッセージの長さ、およびメッセージが保持されます。TAC のデバッグツールでは、HTTPS、管理者のユーザ名とパスワード、および指定された日付を使用して、キャプチャされたパケットを保持している暗号化済みファイルを1つだけ要求します。同様にこのツールでは、暗号化ファイルを復号化するためのキー情報を要求します。 <p>ヒント TACにお問い合わせいただく前に、該当するデバイス間でスニファトレースを使用して、SRTPパケットをキャプチャする必要があります。</p>
<p>[パケットキャプチャ時間 (Packet Capture Duration)]</p>	<p>この設定値は、暗号化のトラブルシューティングを行う場合にだけ使用します。パケットキャプチャを実行すると、CPUの使用率が上昇して、コール処理が妨げられる可能性があります。</p> <p>このフィールドには、1つのパケットキャプチャセッションに割り当てる時間の上限 (分単位) を指定します。デフォルト設定は0で、範囲は0 ~ 300分です。</p> <p>パケットキャプチャを開始するには、フィールドに0以外の値を入力します。パケットキャプチャが完了すると、値0が表示されます。</p>

関連トピック

[ゲートウェイの設定 (Gateway Configuration)]ウィンドウおよび[トランクの設定 (Trunk Configuration)]ウィンドウでのパケットキャプチャの設定 (543 ページ)

[電話の設定 (Phone Configuration)] ウィンドウでのパケット キャプチャの設定 (542 ページ)

キャプチャしたパケットの分析

Cisco Technical Assistance Center (TAC) は、デバッグ ツールを使用してパケットを分析します。TAC にお問い合わせいただく前に、該当するデバイス間でスニファトレースを使用して、SRTP パケットをキャプチャしてください。次の情報を収集したら、TAC に直接お問い合わせください。

- パケット キャプチャ ファイル : `https://<IP アドレスまたはサーバ名>/pktCap/pktCap.jsp?file=mm-dd-yyyy.pkt`。サーバを参照し、西暦年と日付 (mm-dd-yyyy) 別のパケット キャプチャ ファイルを見つけます。
- ファイルのキー : `https://<IP アドレスまたはサーバ名>/pktCap/pktCap.jsp?key=mm-dd-yyyy.pkt`。サーバを参照し、西暦年と日付 (mm-dd-yyyy) 別のキーを見つけます。
- Standard Packet Sniffer Users グループに所属しているエンド ユーザのユーザ名とパスワード。

詳細については、[Cisco Unified Communications Manager セキュリティ ガイド](#) を参照してください。

一般的なトラブルシューティングのタスク、ツール、およびコマンド

この項では、ルート アクセスが無効にされた Unified Communications Manager サーバのトラブルシューティングに役立つコマンドやユーティリティのクイック リファレンスを提供します。次の表に、システムのさまざまな問題をトラブルシューティングするための情報収集に使用できる CLI コマンドと GUI をまとめます。

表 95: CLI コマンドと GUI のまとめ

情報	Linux コマンド	サービスアビリティの GUI ツール	CLI コマンド
CPU 使用率	top	RTMT [表示 (View)] タブに移動し、 [サーバ (Server)] > [CPU とメモリ (CPU and Memory)] を選択	プロセッサ CPU 使用率 : show perf query class Processor すべてのプロセスのプロセス CPU 使用率 : show perf query counter Process 「% CPU Time」 個々のプロセスカウンタの詳細 (CPU 使用率を含む) show perf query instance <Process task_name>
プロセス状態	ps	RTMT [表示 (View)] タブに移動し、 [サーバ (Server)] > [プロセス (Process)] を選択	show perf query counter Process 「Process Status」
ディスク使用量	df/du	RTMT [表示 (View)] タブに移動し、 [サーバ (Server)] > [ディスク使用量 (Disk Usage)] を選択	show perf query counter Partition 「% Used」 または show perf query class Partition
メモリ	free	RTMT [表示 (View)] タブに移動し、 [サーバ (Server)] > [CPU とメモリ (CPU and Memory)] を選択	show perf query class Memory
Network ステータス	netstats		show network status
サーバのリブート	reboot	サーバの [プラットフォーム (Platform)] Web ページにログイン [サーバ (Server)] > [現在のバージョン (Current Version)] に移動	utils system restart

情報	Linux コマンド	サービスアビリティの GUI ツール	CLI コマンド
トレース/ログの収集	Sftp、ftp	RTMT [ツール (Tools)] タブに移動し、[トレース (Trace)]>[トレースおよびログ セントラル (Trace & Log Central)] を選択	ファイルのリスト : file list ファイルのダウンロード : file get ファイルの表示 : file view

次の表に、一般的な問題と、そのトラブルシューティングに使用するツールのリストを示します。

表 96: CLI コマンドおよび GUI 選択オプションによる一般的な問題のトラブルシューティング

タスク	GUI ツール	CLI コマンド
データベースにアクセスする	none	admin としてログインし、次のいずれかの show コマンドを使用します。 <ul style="list-style-type: none"> • show tech database • show tech dbinuse • show tech dbschema • show tech devdefaults • show tech gateway • show tech locales • show tech notify • show tech procedures • show tech routepatterns • show tech routeplan • show tech systables • show tech table • show tech triggers • show tech version • show tech params* <p>SQL コマンドを実行するには、run コマンドを使用します。</p> <ul style="list-style-type: none"> • run sql <sql command>

タスク	GUI ツール	CLI コマンド
ディスクの空き容量を増やす (注) Log パーティションにあるファイルだけ、削除できます。	RTMT クライアントアプリケーションを使用して、[ツール (Tools)] タブに移動し、[トレースおよびログ セントラル (Trace & Log Central)] > [ファイルの収集 (Collect Files)] を選択します。 収集するファイルの選択基準を選択し、[ファイルの削除 (Delete Files)] オプションのチェックボックスをオンにします。この操作を実行すると、ファイルが PC にダウンロードされ、Unified Communications Manager サーバ上のファイルは削除されます。	file delete
コア ファイルを表示する	コアファイルは表示できませんが、RTMT アプリケーションを使用して [Trace & Log Central] > [クラッシュ ダンプの収集 (Collect Crash Dump)] を選択すると、コア ファイルをダウンロードできます。	utils core [options]
Unified Communications Manager サーバをリポートする	サーバの [プラットフォーム (Platform)] ページにログインし、[リスタート (Restart)] > [現在のバージョン (Current Version)] に移動します。	utils system restart
トレースのデバッグレベルを変更する	https://<server_ipaddress>:8443/ccmservice// で <i>Cisco Unity Connection Serviceability Administration</i> にログインして、[トレース (Trace)] > [設定 (Configuration)] を選択します。	set trace enable [Detailed, Significant, Error, Arbitrary, Entry_exit, State_Transition, Special] [syslogmib, cdpmib, dbl, dbnotify]
ネットワークのステータスを表示する	none	show network status

トラブルシューティングのヒント

次の各ヒントは、Unified Communications Manager のトラブルシューティングに役立ちます。



ヒント Unified Communications Manager のリリース ノートで既知の問題を確認します。リリース ノートには、既知の問題の説明と対応策が記載されています。



ヒント デバイスの登録先を確認します。

各 Unified Communications Manager ログはファイルをローカルでトレースします。電話機またはゲートウェイが特定の Unified Communications Manager に登録されている場合、その Unified Communications Manager でコールが開始されると、コール処理はそこで実行されます。問題をデバッグするには、その Unified Communications Manager 上のトレースを取り込む必要があります。

デバイスがサブスクライバ サーバに登録されているにもかかわらず、パブリッシャ サーバ上のトレースを取り込むという間違いがよくあります。そのトレースファイルはほとんど空です（そのファイルには目的のコールが含まれていません）。

デバイス 1 を CM1 に登録し、デバイス 2 を CM2 に登録しているために問題が生じることも多くあります。デバイス 1 がデバイス 2 をコールすると CM1 でコールトレースが実行され、デバイス 2 がデバイス 1 をコールすると CM2 でトレースが実行されます。双方向のコール問題のトラブルシューティングを行う場合は、トラブルシューティングに必要なすべての情報を得るために、両方の Unified Communications Manager からの両方のトレースが必要となります。



ヒント 問題のおおよその時刻を確認します。

複数のコールが発信された可能性があるため、コールのおおよその時刻を確認していると、TAC が問題を迅速に特定するのに役立ちます。

Cisco Unified IP Phone 79xx の電話機統計情報は、**i** または **?** ボタンをアクティブ コール中に 2 回押すと取得できます。

テストを実行して問題を再現し、情報を生成する場合は、問題を理解するために不可欠な次のデータを確認してください。

- 発信側の番号または着信側の番号
- 特定のシナリオに関係する他の番号
- コールの時刻



(注) トラブルシューティングには、すべての機器の時刻が同期化されていることが重要であることに注意してください。

問題を再現している場合は、ファイルの変更日付とタイムスタンプを調べて、その時間枠のファイルを選択します。適切なトレースを収集する最良の方法は、問題を再現してからすぐに最新のファイルを見つけ、そのファイルを Unified Communications Manager サーバからコピーすることです。



ヒント ログ ファイルを保存して、上書きされないようにします。

ファイルは、時間が経つと上書きされます。ログが記録されているファイルを調べる唯一の方法は、メニューバーで [表示 (View)] > [更新 (Refresh)] を選択し、ファイルの日付と時刻を確認することです。

システム履歴ログ

システム履歴ログを使用すると、システムの初期インストール、システムのアップグレード、Cisco オプションのインストール、DRS バックアップと DRS 復元、バージョン切り替えとリブート履歴などの情報の概要を中央からすばやく把握できます。

関連トピック

[システム履歴ログの概要](#) (552 ページ)

[システム履歴ログのフィールド](#) (553 ページ)

[システム履歴ログへのアクセス](#) (554 ページ)

システム履歴ログの概要

システム履歴ログは、**system-history.log** という単純な ASCII ファイルとして保管され、そのデータはデータベース内には保持されません。サイズが膨大ではないため、ローテーションされることはありません。

システム履歴ファイルには、次の機能があります。

- サーバ上のソフトウェアの初期インストールを記録します。
- ソフトウェアの各アップデート (Cisco オプションファイルおよびパッチ) の成功、失敗、またはキャンセルを記録します。
- 実行される各 DRS バックアップと復元を記録します。
- CLI または GUI によって発行されるバージョン切り替えの各呼び出しを記録します。
- CLI または GUI によって発行される再起動およびシャットダウンの各呼び出しを記録します。
- システムの各ブートを記録します。再起動エントリまたはシャットダウンエントリと関連付けられていない場合のブートは、手動リブート、電源サイクル、またはカーネルパニックの結果として発生したものです。

- 初期インストール以降、または機能が利用可能になって以降のシステム履歴を単一ファイルに保持します。
- インストールフォルダに存在します。 **file** コマンドか、または Real Time Monitoring Tool (RTMT) を使用して、CLI からログにアクセスできます。

システム履歴ログのフィールド

ログには、製品名、製品バージョン、およびカーネルイメージに関する情報を含む、次のような共通のヘッダーが表示されます。

```
=====
Product Name - Unified Communications Manager
Product Version - 7.1.0.39000-9023
Kernel Image - 2.6.9-67.EL
=====
```

システム履歴ログの各エントリには、次のようなフィールドがあります。

timestamp userid action description start/result

システム履歴ログのフィールドには、次のような値が含まれます。

- *timestamp* : サーバ上のローカルな日付と時刻が *mm/dd/yyyy hh:mm:ss* の形式で表示されます。
- *userid* : アクションを呼び出したユーザの名前が表示されます。
- *action* : 次のいずれかのアクションが表示されます。
 - インストールするもの
 - Windows アップグレード
 - インストール時のアップグレード
 - アップグレード
 - Cisco オプションのインストール
 - バージョン切り替え
 - システム再起動
 - シャットダウン
 - Boot
 - DRS バックアップ
 - DRS 復元
- *description* : 次のいずれかのメッセージが表示されます。

- **Version** : 基本インストール、Windows アップグレード、インストール時のアップグレード、アップグレードの各アクションが表示されます。
 - **Cisco Option file name** : Cisco オプションのインストールのアクションが表示されます。
 - **Timestamp** : DRS バックアップと DRS 復元の各アクションが表示されます。
 - **Active version to inactive version** : バージョン切り替えのアクションが表示されます。
 - **Active version** : システム再起動、シャットダウン、およびブートの各アクションが表示されます。
- **result** : 次の結果が表示されます。
 - 開始
 - 成功または失敗
 - キャンセル

次に、システム履歴ログの例を示します。

```
admin:file dump install system-history.log=====
Product Name - Cisco Unified Communications Manager Product Version -
6.1.2.9901-117 Kernel Image - 2.4.21-47.EL.cs.3BOOT
===== 07/25/2008 14:20:06 | root: Install
6.1.2.9901-117 Start 07/25/2008 15:05:37 | root: Install 6.1.2.9901-117 Success
07/25/2008 15:05:38 | root: Boot 6.1.2.9901-117 Start 07/30/2008 10:08:56 |
root: Upgrade 6.1.2.9901-126 Start 07/30/2008 10:46:31 | root: Upgrade
6.1.2.9901-126 Success 07/30/2008 10:46:43 | root: Switch Version 6.1.2.9901-117
to 6.1.2.9901-126 Start 07/30/2008 10:48:39 | root: Switch Version
6.1.2.9901-117 to 6.1.2.9901-126 Success 07/30/2008 10:48:39 | root: Restart
6.1.2.9901-126 Start 07/30/2008 10:51:27 | root: Boot 6.1.2.9901-126 Start
08/01/2008 16:29:31 | root: Restart 6.1.2.9901-126 Start 08/01/2008 16:32:31
| root: Boot 6.1.2.9901-126 Start
```

システム履歴ログへのアクセス

システム履歴ログにアクセスするには、CLI または RTMT を使用できます。

CLI の使用

次のように CLI の **file** コマンドを使用すると、システム履歴ログにアクセスできます。

- **file view install system-history.log**
- **file get install system-history.log**

CLI ファイル コマンドの詳細については、『*Command Line Interface Reference Guide for Cisco Unified Communications Solutions*』を参照してください。

RTMT の使用

RTMT を使用してシステム履歴ログにアクセスすることもできます。[Trace and Log Central] タブで、[インストール ログの収集 (Collect Install Logs)] を選択します。

RTMT の使用の詳細については、『*Cisco Unified Real-Time Monitoring Tool Administration Guide*』を参照してください。

監査ロギング

集中型監査ログによって、Unified Communications Manager システムの設定の変更が個別の監査ログファイルに記録されます。監査イベントは、記録する必要があるすべてのイベントを指します。次の Unified Communications Manager コンポーネントによって監査イベントが生成されます。

- Cisco Unified Communications Manager Administration
- Cisco Unified Serviceability
- *Unified Communications Manager CDR Analysis and Reporting*
- *Cisco Real-Time Monitoring Tool*
- *Cisco Unified Communications Operating System*
- *Disaster Recovery System*
- データベース
- コマンドライン インターフェイス
- Remote Support Account Enabled (テクニカル サポート チームによって発行される CLI コマンド)

Cisco Business Edition 5000 では、次の Cisco Unity Connection コンポーネントによっても監査イベントが生成されます。

- Cisco Unity Connection の管理
- *Cisco Personal Communications Assistant* (Cisco PCA)
- Cisco Unity Connection Serviceability
- Representational State Transfer (REST) API を使用する Cisco Unity Connection クライアント

次に、監査イベントの例を示します。

```
CCM_TOMCAT-GENERIC-3-AuditEventGenerated: Audit Event Generated
UserID:CCMAdministrator Client IP Address:172.19.240.207 Severity:3
EventType:ServiceStatusUpdated ResourceAccessed: CCMService
EventStatus:Successful Description: Call Manager Service status is stopped App
ID:Cisco Tomcat Cluster ID:StandAloneCluster Node ID:sa-cm1-3
```

監査イベントに関する情報が含まれている監査ログは、共通のパーティションに書き込まれます。これらの監査ログのパーティションは、トレースファイルと同様に、Log Partition Monitor (LPM) によって管理されます。デフォルトでは、LPM によって監査ログがパーティションされますが、監査ユーザは Cisco Unified Serviceability の [Audit User Configuration] ウィンドウからこの設定を変更できます。共通パーティションのディスク使用量がしきい値を超えると、LPM によってアラートが送信されますが、アラートには、ディスクが監査ログまたはトレースファイルによっていっぱいであるかどうかに関する情報は含まれていません。



ヒント 監査ログをサポートするネットワークサービスである Cisco Audit Event Service は、Cisco Unified Serviceability のコントロールセンターのネットワークサービスに表示されます。監査ログへの書き込みが行われない場合は、Cisco Unified Serviceability で [Tools] > [Control Center-Network Services] を選択し、このサービスを停止してから開始します。

すべての監査ログは、Cisco Unified Real-Time Monitoring Tool の Trace and Log Central から収集、表示、および削除します。RTMT の Trace and Log Central で監査ログにアクセスします。[システム (System)] > [リアルタイム トレース (Real-Time Trace)] > [監査ログ (Audit Logs)] > [ノード (Nodes)] に移動します。ノードを選択したら、別のウィンドウに [システム (System)] > [Cisco 監査ログ (Cisco Audit Logs)] が表示されます。

RTMT には、次のタイプの監査ログが表示されます。

- アプリケーション ログ
- 問い合わせや
- オペレーティング システム ログ
- リモート SupportAccEnabled ログ

アプリケーション ログ

RTMT の AuditApp フォルダに表示されるアプリケーション監査ログには、Cisco Unified Communications Manager Administration、Cisco Unified Serviceability、CLI、Cisco Unified リアルタイム監視ツール (RTMT)、ディザスタリカバリ システム、および Cisco Unified CDR Analysis and Reporting (CAR) の設定変更が記録されます。Cisco Business Edition 5000 の場合、アプリケーション監査ログには Cisco Unity Connection の管理、Cisco Personal Communications Assistant (Cisco PCA)、Cisco Unity Connection のサービスアビリティ、および Representational State Transfer (REST) API を使用するクライアントに対する変更も記録されます。

アプリケーション ログはデフォルトは有効になっていますが、Cisco Unified Serviceability で [Tools] > [Audit Log Configuration] を選択することによって設定を変更できます。設定可能な監査ログの設定については、『Cisco Unified Serviceability Administration Guide』を参照してください。

Cisco Unified Serviceability で監査ログがディセーブルになると、新しい監査ログは作成されません。



ヒント 監査のロールを割り当てられたユーザだけが監査ログの設定を変更する権限を持っています。新規のインストールまたはアップグレード後には、デフォルトで **CCMAdministrator** に監査のロールが割り当てられます。**CCMAdministrator** は、監査のために作成した新規ユーザを「**Standard Audit Users**」グループに割り当てることができます。その後、**CCMAdministrator** を監査ユーザグループから削除できます。「**Standard Audit Log Configuration**」ロールには、監査ログを削除する権限と、*Cisco Unified Real-Time Monitoring Tool*、Trace Collection Tool、RTMT Alert Configuration、[コントロールセンターのネットワーク サービス (Control Center - Network Services)] ウィンドウ、RTMT Profile Saving、[監査の設定 (Audit Configuration)] ウィンドウ、および Audit Traces という新規リソースへの読み取り/更新権限が与えられます。*Cisco Business Edition 5000* の Cisco Unity Connection の場合、インストール時に作成されたアプリケーション管理アカウントは、**Audit Administrator** ロールに割り当てられます。このアカウントは、他の管理者ユーザをこのロールに割り当てることができます。

Unified Communications Manager では、1つのアプリケーション監査ログファイルが作成され、設定済みの最大ファイルサイズに到達すると、そのファイルが閉じられて新しいアプリケーション監査ログファイルが作成されます。システムでログファイルのローテーションが指定されている場合は、**Unified Communications Manager** によって設定済みの数のファイルが保存されます。ログイベントの一部は、**RTMT SyslogViewer** を使用して表示できます。

Cisco Unified Communications Manager Administration では、次のイベントが記録されます。

- ユーザのログイン/ログアウト。
- ユーザのロールメンバーシップの更新 (ユーザの追加、ユーザの削除、またはユーザのロールの更新)
- ロールの更新 (新しいロールの追加、削除、または更新)
- デバイスの更新 (電話機およびゲートウェイ)
- サーバ設定の更新 (アラームまたはトレースの設定、サービスパラメータ、エンタープライズパラメータ、IP アドレス、ホスト名、イーサネット設定の変更、および **Unified Communications Manager** サーバの追加または削除)

Cisco Unified Serviceability では、次のイベントが記録されます。

- サービスアビリティ ウィンドウからのサービスのアクティブ化、非アクティブ化、開始、または停止。
- トレース設定およびアラーム設定の変更。
- SNMP 設定の変更。
- CDR 管理の変更。
- サービスアビリティ レポートのアーカイブのレポートの参照。このログはレポーターノードで表示します。

RTMT では、次のイベントが監査イベントアラームとともに記録されます。

- アラートの設定。
- アラートの中断。
- 電子メールの設定。
- ノードアラート ステータスの設定。
- アラートの追加。
- アラートの追加アクション。
- アラートのクリア。
- アラートのイネーブル化。
- アラートの削除アクション。
- アラートの削除。

Unified Communications Manager CDR Analysis and Reporting では、次のイベントが記録されます。

- CDR ローダのスケジュール
- 日次、週次、月次のユーザ レポート、システム レポート、およびデバイス レポートのスケジュール
- メール パラメータの設定
- ダイアル プランの設定
- ゲートウェイの設定
- システム プリファレンスの設定
- 自動消去の設定
- 接続時間、時刻、および音声品質の評価エンジンの設定
- QoS の設定
- 事前生成レポートの自動生成/アラートの設定
- 通知限度の設定

ディザスタ リカバリ システムでは、次のイベントが記録されます。

- 開始に成功または失敗したバックアップ
- 開始に成功または失敗した復元
- 正しくキャンセルされたバックアップ
- 完了に成功または失敗したバックアップ
- 完了に成功または失敗した復元

- バックアップ スケジュールの保存、更新、削除、イネーブル化、ディセーブル化
- バックアップの宛先デバイスの保存、更新、削除

Cisco Business Edition 5000 の場合、Cisco Unity Connection の管理では、次のイベントが記録されます。

- ユーザのログイン/ログアウト。
- すべての設定変更（ユーザ、連絡先、コール管理オブジェクト、ネットワーク、システム設定、テレフォニーなど）。
- タスク管理（タスクの有効化/無効化）。
- 一括管理ツール（一括作成、一括削除）。
- カスタム キーパッド マップ（マップの更新）

Cisco Business Edition 5000 の場合、Cisco PCA では、次のイベントが記録されます。

- ユーザのログイン/ログアウト。
- Messaging Assistant で行われたすべての設定変更。

Cisco Business Edition 5000 の場合、Cisco Unity Connection Serviceability では、次のイベントが記録されます。

- ユーザのログイン/ログアウト。
- すべての設定変更。
- サービスのアクティブ化、非アクティブ化、開始、または停止。

Cisco Business Edition 5000 の場合、REST API を使用するクライアントでは、次のイベントが記録されます。

- ユーザのログイン（ユーザの API 認証）。
- Cisco Unity Connection プロビジョニング インターフェイス（CUPI）を使用する API 呼び出し。

データベース ログ

RTMT の *informix* フォルダに表示されるデータベース監査ログでは、データベースの変更がレポートされます。このログは、デフォルトでは有効になっていませんが、Cisco Unified Serviceability で **[Tools] > [Audit Log Configuration]** を選択することによって設定を変更できます。設定可能な監査ログの設定については、Cisco Unified Serviceability を参照してください。

このログは、アプリケーションの設定変更を記録するアプリケーション監査ログとは異なり、データベースの変更を記録します。Cisco Unified Serviceability でデータベース監査がイネーブルに設定されるまで、*informix* フォルダは RTMT に表示されません。

オペレーティング システム ログ

RTMT の vos フォルダに表示されるオペレーティング システム 監査ログでは、オペレーティング システムによってトリガーされるイベントがレポートされます。デフォルトでは、イネーブルになっていません。utils auditd CLI コマンドによって、イネーブルまたはディセーブルにしたり、イベントのステータスを提供したりできます。

CLI で監査がイネーブルに設定されるまで、vos フォルダは RTMT に表示されません。

CLI の詳細については、『*Command Line Interface Reference Guide for Cisco Unified Solutions*』を参照してください。

リモート サポート アカウントイネーブル化ログ

RTMT の vos フォルダに表示されるリモート サポート アカウント イネーブル化ログでは、テクニカル サポート チームによって発行される CLI コマンドがレポートされます。このログの設定は変更できません。このログは、テクニカル サポート チームによってリモート サポート アカウントがイネーブルに設定された場合にだけ作成されます。

Cisco Unified Communications Manager サービスが稼働しているかどうかの確認

サーバ上で Cisco CallManager サービスがアクティブであることを確認するには、次の手順を実行します。

手順

1. Cisco Unified Communications Manager Administration で、[ナビゲーション (Navigation)] > [Cisco Unified Serviceability] を選択します。
2. [ツール (Tools)] > [サービス アクティベーション (Service Activation)] を選択します。
3. [サーバ (Server)] カラムから必要なサーバを選択します。

選択したサーバが [現在のサーバ (Current Server)] というタイトルの隣に表示され、設定済みのサービスを示す一連のボックスが表示されます。

Cisco CallManager 行の [アクティベーション ステータス (Activation Status)] カラムに、[アクティブ化 (Activated)] または [非アクティブ (Deactivated)] と表示されます。

[アクティブ化 (Activated)] というステータスが表示されている場合、選択したサーバ上で、指定した Cisco CallManager サービスがアクティブのままになっています。

[非アクティブ (Deactivated)] というステータスが表示されている場合は、引き続き次のステップを実行します。

4. 目的の Cisco CallManager サービスのチェックボックスをオンにします。
5. [更新 (Update)] ボタンをクリックします。

指定した Cisco CallManager サービス行の [アクティベーション ステータス (Activation Status)] カラムに [アクティブ化 (Activated)] と表示されます。

これで、選択したサーバ上の指定したサービスがアクティブになります。

Cisco CallManager サービスがアクティブであるかどうか、およびサービスが現在動作しているかどうかを確認するには、次の手順を実行します。

手順

1. Cisco Unified Communications Manager Administration で、[ナビゲーション (Navigation)] > [Cisco Unified Serviceability] を選択します。

[Cisco Unified Serviceability] ウィンドウが表示されます。

2. [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)] を選択します。

3. [サーバ (Server)] カラムからサーバを選択します。

選択したサーバが **Current Server** というタイトルの隣に表示され、設定済みのサービスを示すボックスが表示されます。

[ステータス (Status)] カラムに、選択したサーバでどのサービスが動作しているかが表示されます。



第 38 章

TAC とのケースのオープン

この項では、TAC に問い合わせる場合に必要な情報の詳細、および TAC の担当者と情報を共有する方法について説明します。

シスコテクニカルサポートでは、有効なシスコサービス契約を保有しているすべてのお客様、パートナー、リセラー、およびディストリビュータ向けに、24時間対応の高い評価を得ているテクニカルサポートを用意しています。Cisco Technical Support Web サイトでは、シスコ製品やシスコテクノロジーに関する技術的な問題を解決するためのオンラインのドキュメントやツールをご利用いただけます。この Web サイトは、1 年中いつでも利用することができます。次の URL にアクセスしてください。<http://www.cisco.com/techsupport>

オンラインの TAC Service Request Tool を使用すると、S3 と S4 のサービス リクエストを短時間でオープンできます。(S3 と S4 の問題とは、ネットワークの障害が軽微である場合、あるいは製品情報が必要な場合を意味します)。状況をご説明いただくと、TAC Service Request ツールが自動的に推奨する解決方法を提供します。これらの推奨手段で問題を解決できない場合は、Cisco TAC のエンジニアが対応します。次の URL から、TAC サービス リクエスト ツールにアクセスできます。<http://www.cisco.com/techsupport/servicerequest>

S1 または S2 サービス要求の場合、またはインターネットにアクセスできない場合、電話で Cisco TAC にご連絡ください (S1 または S2 の問題とは、運用中のネットワークがダウンした場合、あるいは重大な障害が発生した場合を意味します)。S1 および S2 の問題には Cisco TAC の技術者がただちに対応し、業務を円滑に実行できるよう支援します。

電話でサービス要求を利用するには、次のいずれかの番号におかけください。

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)

EMEA: +32 2 704 55 55

米国 : 1 800 553 2447

Cisco TAC の連絡先一覧は、<http://www.cisco.com/techsupport/contacts> で確認できます。

- [必要な情報 \(564 ページ\)](#)
- [必要な予備的情報 \(564 ページ\)](#)
- [TAC Case Open ツールのオンライン サービス \(566 ページ\)](#)
- [Serviceability Connector \(566 ページ\)](#)
- [Cisco Live! \(567 ページ\)](#)

- [リモートアクセス](#) (568 ページ)
- [Cisco Secure Telnet](#) (568 ページ)
- [リモートアカウントの設定](#) (570 ページ)

必要な情報

Cisco TAC に対してサービス リクエストをオープンする場合は、問題を特定し、その内容を把握しやすくするための予備的信息をご提供いただく必要があります。問題の内容によっては、追加の情報をご提供いただく必要があります。次に示す情報をエンジニアから要求されなくても遅滞なく収集してください。サービス リクエストをオープンし、エンジニアから要求されたあとに収集を開始すると、問題の解決が遅くなります。

関連トピック

- [Cisco Live!](#) (567 ページ)
- [Cisco Secure Telnet](#) (568 ページ)
- [一般情報](#) (565 ページ)
- [ネットワーク レイアウト](#) (564 ページ)
- [TAC Case Open ツールのオンライン サービス](#) (566 ページ)
- [問題の説明](#) (565 ページ)
- [リモートアクセス](#) (568 ページ)
- [必要な予備的信息](#) (564 ページ)

必要な予備的信息

すべての問題において、必ず次の情報を TAC に提供してください。この情報を収集および保存して TAC サービス リクエストをオープンするときに使用できるようにし、変更があった場合には定期的に更新します。

関連トピック

- [一般情報](#) (565 ページ)
- [ネットワーク レイアウト](#) (564 ページ)
- [問題の説明](#) (565 ページ)

ネットワーク レイアウト

物理セットアップおよび論理セットアップの詳細な説明、および音声ネットワークに関連する次のすべてのネットワーク要素をお知らせください (存在する場合)。

- Unified Communications Manager
 - バージョン (Unified Communications Manager Administration で **[詳細 (Details)]** を選択)
 - Unified Communications Manager の数

- セットアップ (スタンドアロン、クラスタ)
 - Unity[Unity]
- バージョン (Unified Communications Manager Administration から)
- 統合のタイプ
 - アプリケーション
- インストールされているアプリケーションのリスト
- 各アプリケーションのバージョン番号
 - IP/音声ゲートウェイ
- OS のバージョン
- show tech コマンド (IOS ゲートウェイ)
- Unified Communications Manager の負荷 (Skinny ゲートウェイ)
 - スイッチ
- OS のバージョン
- VLAN の設定
 - ダイヤルプラン : 番号付け方式、コールルーティング

Visio や JPG などで作成した詳細な図を提出すると理想的です。ホワイトボードを使用して、Cisco Live! セッションから図を提供することもできます。

問題の説明

問題が発生したときにユーザが実行した処理について、手順ごとの詳細を提供します。詳細情報には、次の内容を含める必要があります。

- 予想される動作
- 実際に観察された動作の詳細

一般情報

次の情報を準備する必要があります。

- 新しいインストールかどうか

- 以前のバージョンの Unified Communications Manager がインストールされている場合、最初からこの問題が発生していたかどうか（最初から発生していない場合は、最近システムに対して行った変更）
- この問題は再現可能かどうか
 - 再現可能である場合は、通常的环境で発生するか、または特別な環境で発生するか
 - 再現不可能である場合は、問題発生のタイミングが特別であったかどうか
 - 発生の頻度
- 影響のあるデバイス
 - ランダムなデバイスではなく、特定のデバイスが影響を受ける場合、影響を受けるデバイスの共通点は何か
 - 問題に関連するすべてのデバイスの DN または IP アドレス（ゲートウェイの場合）
- コールパス上のデバイス（存在する場合）

TAC Case Open ツールのオンライン サービス

Cisco.com から TAC Case Open ツールのオンライン サービスを使用すると、他のすべてのサービス リクエスト オープン方法よりも優先的に処理されます。ただし、高優先度のサービス リクエスト（P1 および P2）は例外です。

サービス リクエストをオープンする場合は、問題についての正確な説明を提供してください。問題の説明を提供すると、すぐに解決策として使用できる可能性がある URL リンクが返されます。

リンクを参照しても問題の解決策が見つからない場合は、プロセスを続行して、サービス リクエストを TAC エンジニアに送信してください。

Serviceability Connector

Serviceability Connector の概要

Webex Serviceability サービスを使用すると、ログの収集を容易にすることができます。このサービスでは、診断ログと情報を検索、取得して、タスクを自動化します。

この機能は、オンプレミスで導入された有用性コネクタを使用します。有用性コネクタは、ネットワーク内の専用のネットワーク（「コネクタホスト」）で実行されます。コネクタは、次のいずれかのコンポーネントに取り付けることができます。

- エンタープライズ コンピューティング プラットフォーム（ECP） - 推奨

ECPは、**Docker** コンテナを使用して、サービスを分離、保護、および管理します。ホストと有用性コネクタアプリケーションはクラウドからインストールされます。最新かつ安全な状態を維持するために、手動でアップグレードする必要はありません。



重要 ECPの使用を推奨します。私たちの将来の開発は、このプラットフォームに焦点を当てます。Expresswayに有用性コネクタをインストールすると、一部の新機能が使用できなくなります。

- Cisco Expressway

次の目的で有用性コネクタを使用できます。

- サービスリクエストの自動ログおよびシステム情報取得
- クラウドに接続されている UC 展開での Unified CM クラスタのログ収集

両方のユースケースで同じ有用性コネクタを使用できます。

Serviceability サービスを使用する利点

このサービスには次の利点があります。

- ログの収集を高速化します。TACエンジニアは、問題の診断を実行する際に関連するログを取得できます。追加のログを要求し、手動での収集と配信を待機する遅延を回避できます。この自動化により、問題解決にかかる時間を数日にすることができます。
- TAC の Collaboration Solution Analyzer および診断シグニチャのデータベースと連携します。システムは自動的にログを分析し、既知の問題を特定して、既知の修正または回避策を推奨します。

Serviceability Connector の TAC サポート

有用性コネクタの詳細については<https://www.cisco.com/go/serviceability>、を参照するか、TACの担当者にお問い合わせください。

Cisco Live!

安全で暗号化された Java アプレットである Cisco Live! を利用すると、コラボレーティブ Web ブラウジング、URL 共有、ホワイトボード、Telnet、クリップボードツールを使用することによって、Cisco TAC のエンジニアとより効率的に協同して作業できます。

Cisco Live にアクセスします。次の URL にあります。

<http://c3.cisco.com/>

リモート アクセス

リモート アクセスを使用すると、必要なすべての装置に対して Terminal Services セッション（リモート ポート 3389）、HTTP セッション（リモート ポート 80）、および Telnet セッション（リモート ポート 23）を確立できます。



注意 ダイヤルインを設定する場合は、システムに対する脆弱性となるため、**login:cisco** または **password:cisco** は使用しないでください。

TAC エンジニアが次のいずれかの方法を使用してデバイスにリモート アクセスすることを許可すると、多くの問題を非常に迅速に解決できます。

- パブリック IP アドレスが設定された装置
- ダイヤルインアクセス：（プリファレンスの高い順に）アナログ モデム、統合デジタル通信網（ISDN）モデム、バーチャルプライベートネットワーク（VPN）
- ネットワークアドレス変換（NAT）：プライベート IP アドレスが設定された装置へのアクセスを可能にする IOS およびプライベートインターネットエクステンジ（PIX）。

エンジニアの介入時にファイアウォールによって IOS トラフィックと PIX トラフィックが遮断されないこと、およびサーバ上で Terminal Services などの必要なすべてのサービスが開始されていることを確認してください。



(注) TAC では、すべてのアクセス情報は厳重に管理されます。また、お客様の同意なしにシステムを変更することはありません。

Cisco Secure Telnet

Cisco Secure Telnet は、Cisco Service Engineers（CSE）がトランスペアレントファイアウォールを使用してユーザのサイトにある Unified Communications Manager サーバにアクセスできる機能を提供します。

Cisco Secure Telnet は、シスコのファイアウォール内部で Telnet クライアントをイネーブル化することによって、ファイアウォールで稼働する Telnet デーモンに接続します。このセキュアな接続により、ファイアウォールの変更を行わずに Unified Communications Manager サーバをリモートモニタリングおよびメンテナンスできます。



(注) シスコは、許可があった場合にだけお客様のネットワークにアクセスします。サイトに、このプロセスの開始を支援するネットワーク管理者を配置する必要があります。

ファイアウォールによる保護

ほとんどすべての内部ネットワークでは、外部から内部のホストシステムへのアクセスを制限するためにファイアウォールアプリケーションが使用されています。これらのアプリケーションでは、ネットワークとパブリックインターネットとの間のIP接続を制限することによって、ネットワークが保護されます。

ファイアウォールでは、許可するように明示的に再設定しないかぎり、外部から開始されるTCP/IP接続が自動的にブロックされます。

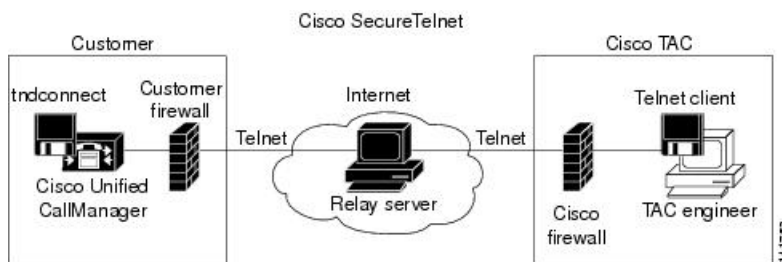
通常、企業ネットワークではパブリックインターネットとの通信が許可されますが、ファイアウォール内部から外部ホストに向けて開始される接続だけが許可されます。

Cisco Secure Telnet の設計

Cisco Secure Telnet では、ファイアウォールの内側から簡単に Telnet 接続を開始できるという技術を活用しています。外部のプロキシマシンを使用して、ファイアウォールの内側からのTCP/IP通信が Cisco Technical Assistance Center (TAC) にある別のファイアウォールの内側のホストへとリレーされます。

このリレーサーバを使用することによって、両方のファイアウォールの完全性が維持され、また保護されたリモートシステム間の安全な通信がサポートされます。

図 26: Cisco Secure Telnet システム



Cisco Secure Telnet の構造

外部のリレーサーバによって、お客様のネットワークとシスコとの間に Telnet トンネルが構築され、接続が確立されます。これにより、Unified Communications Manager サーバの IP アドレスとパスワード識別子を CSE に送信できます。



(注) パスワードは、管理者と CSE が相互に同意した文字列です。

管理者は、Telnet トンネルを開始することによって、プロセスを開始します。これにより、ファイアウォールの内部からパブリックインターネット上のリレーサーバへの TCP 接続が確立されます。次に、Telnet トンネルによって、ローカルの Telnet サーバへの別の接続が確立され、エンティティ間の双方向のリンクが作成されます。



- (注) Cisco TAC の Telnet クライアントは、Windows NT および Windows 2000 上で動作するシステム、または UNIX オペレーティング システムに準拠して動作します。

ローカル サイトの Cisco Communications Manager がパスワードを受け入れると、Cisco TAC で実行されている Telnet クライアントは、ローカル ファイアウォールの内側で動作する Telnet デーモンに接続します。この結果確立される透過的接続によって、マシンがローカルで使用されている場合と同様にアクセスできるようになります。

Telnet 接続が安定した後、CSE はすべてのリモート有用性機能の機能を実装して、Unified Communications Manager サーバ上でメンテナンス、診断、およびトラブルシューティングタスクを実行できます。

CSE が送信するコマンド、および Unified Communications Manager サーバから発行される応答を表示することはできますが、コマンドや応答はすべてが完全な形式で表示されるわけではありません。

リモート アカウントの設定

シスコサポートがトラブルシューティングのためにご使用のシステムに一時的にアクセスできるように、Unified Communications Manager でリモート アカウントを設定します。

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)] で、[サービス (Services)] > [リモート サポート (Remote Support)] を選択します。
- ステップ 2 [アカウント名 (Account Name)] フィールドに、リモート アカウントの名前を入力します。
- ステップ 3 [アカウントの有効期限 (Account Duration)] フィールドに、アカウントの有効期限を日数で入力します。
- ステップ 4 [保存 (Save)] をクリックします。
システムは、暗号化パスワードを生成します。
- ステップ 5 シスコのサポート担当者に連絡して、リモート サポート アカウント名とパスワードを提供します。

翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。