Cisco Prime Collaboration Assurance - Advanced and Analytics Guide,12.x(12.1 および 12.1 サービス 梱包 1 つの機能を含む)

初版：2018 年 8 月 8 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.

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)

© 2018 Cisco Systems, Inc. All rights reserved.

目 次

第 I 部 : **Cisco Prime Collaboration の開始** 23

第 1 章 **Cisco Prime Collaboration Assurance および Analytics の概要** 1

Cisco Prime Collaboration Assurance の概要 1

表記法 1

Cisco Prime Collaboration Assurance - Advanced 3

Cisco Prime Collaboration Assurance - Advanced 機能 12

音声とビデオの Unified Dashboard 12

[デバイスインベントリ（Device Inventory）]/[インベントリ管理（Inventory Management）] 13

音声およびビデオのエンドポイント モニタリング 14

診断 15

障害管理 15

レポート 16

IPv6 用の Cisco Prime Collaboration Assurance サポート 16

Cisco Prime Collaboration Assurance の概要 - MSP モード 19

Enterprise モードと MSP モードの違い 24

Cisco Prime Collaboration Assurance NBI 26

Cisco Prime Collaboration Assurance および Analytics の Geo-Redundancy 27

新機能および変更された機能に関する情報 27

Cisco Prime Collaboration Assurance の新機能 30

Cisco Prime Collaboration Analytics の概要 39

Cisco Prime Collaboration Analytics NBI 40

第 2 章 **概要** 43

概要 43
イベント 43
アラーム 44
イベントの作成 44
アラーム作成 45
イベントとアラームの関連付け 46
イベントの集約 47
イベント マスキング 47
アラーム ステータス 47
イベントの重大度 49
イベントおよびアラームのデータベース 49
アラーム通知 49

第 3 章 Cisco Prime Collaboration Assurance を開始する 51
Cisco Prime Collaboration Assurance を開始する 51
Cisco Prime Collaboration Assurance を開始する 51
Cisco Prime Collaboration Analytics の開始 56

第 II 部 : サーバのセットアップ 61

第 4 章 サードパーティ CA 署名付き証明書の有効化 63
サードパーティ CA 署名付き証明書の有効化 63
CA 署名付き証明書のインストール 63

第 5 章 ライセンスの管理 67
ライセンスの管理 67
Cisco Prime Collaboration Assurance のライセンシング 67
Cisco Prime Collaboration Analytics ライセンス 68
Analytics ライセンスの追加 68
Analytics の有効化と無効化 69
Cisco Prime Collaboration Contact Center Assurance のライセンス 69

[ライセンスのカウント（License Count）] 70
Cisco Prime Collaboration Assurance のおよびエンドポイント数 70
ライセンス詳細の表示 71
ライセンス ファイルの追加と削除 73
Cisco Prime Collaboration Assurance で Advanced Evaluation から Advanced（有料ライセンス）に切り替える 73

第 6 章 [ユーザ管理（Manage Users）] 75
[ユーザ管理（Manage Users）] 75
Cisco Prime Collaboration Assurance - 高度なユーザ ロール 75
Cisco Prime Collaboration Assurance のシングル サインオン 77
デフォルト ユーザ アカウント 79
ユーザ ロールおよびタスク 80
ユーザの追加 81
ユーザ ロールの変更 81
LDAP サーバの設定 82
[LDAP Configuration] のパラメータ 83
パスワードの最大数を設定 85
Cisco Prime Collaboration Assurance アカウントのロック解除 86

第 7 章 顧客の管理 87
顧客の管理 87
顧客の追加 87
グローバル顧客の選択 88

第 8 章 ドメインの管理 89
ドメインの管理 89
ドメインの管理 89
アシュアランスドメインの追加 90
グローバルなドメインの選択 90

第 9 章 システム パラメータの設定 91
システム パラメータの設定 91
グローバル システム パラメータ 92
SMTP サーバの設定 94
Cisco Prime Collaboration Assurance サーバのタイム ゾーンの設定 94

第 III 部 : Cisco Prime Collaboration Assurance でのデバイスの管理 97

第 10 章 デバイス クレデンシャルの管理 99
デバイス クレデンシャルの管理 99
デバイス クレデンシャル プロファイルの追加 100
[Credential Profiles] のフィールドの説明 101
デバイス ディスカバリの SSL 証明書認証 118
デバイス クレデンシャルの変更 118
デバイス クレデンシャルの確認 119
クレデンシャル検証のエラー メッセージ 120
デバイス クレデンシャル プロファイルの削除 123

第 11 章 クラスタのセットアップ 125
クラスタのセットアップ 125
Cisco TelePresence Manager、Cisco TMS クラスタ 125

第 12 章 デバイスの検出 129
デバイスの検出 129
ライフ サイクルの検出 129
Cisco Prime Collaboration Assurance の削除時にデバイスを削除 133
検出方法 133
前提条件と推奨事項 142
デバイスの自動検出 150
検出フィルタとスケジュール オプション 154

デバイスの手動検出 157
デバイスのインポート 159
デバイス リストとクレデンシャルのエクスポート 160
トラブルシューティング 161
Cisco Unified Computing System（UCS）の検出 161
vCenter の構成 165
Unified CM クラスタ データの検出 165
クラスタ デバイスの検出をスケジュール 166
デバイスの再検出 168
検出ステータスの確認 169
トラブルシューティング 170

第 13 章 デバイス グループの管理 173
デバイス グループの管理 173
デバイス グループについて 173
グループの作成 177
グループにデバイスを追加 177
グループからデバイスを削除 177
デバイス グループ セレクタ 178

第 14 章 インベントリの管理 179
インベントリの管理 179
インベントリ詳細の表示 179
インベントリ ペイン 180
デバイスの 360° ビュー 186
Cisco Prime Collaboration Assurance のグローバル検索オプション 192
インベントリの概要 195
デバイス ステータスの概要 196
トラブルシューティング 199
インベントリ ステータスのエラー メッセージ 199
デバイス固有のインベントリ詳細 202

インベントリ詳細の更新と収集 218
インベントリの更新 220
ジョブ スケジュール - フィールドの説明 222
インベントリ詳細の収集 222
管理対象デバイスの一時停止と再開 223
デバイスの削除 224
パフォーマンス グラフ 226
Unified CM デバイスの検索 233
SNMP クエリ（SNMP Query） 235

第 15 章 ポーリング デバイス 237
ポーリングの設定 237
概要 237
ポーリング パラメータ：設定 239
ポーリング パラメータの表示 240
ポーリング パラメータの編集 240

第 IV 部： 障害のモニタ 243

第 16 章 通知の設定 245
通知の設定 245
通知グループ 246
通知基準 247
通知の種類 248
SNMP トラップ通知 249
SMTP サーバの設定 257
syslog 通知 257
特定のアラームに制限された通知 259
アラーム セットの追加 259
デバイス通知グループの追加 260
[一般情報（General Information）] フィールドの説明 262

通知先フィールドの説明を設定 263

第 17 章 しきい値ルールの設定 267

しきい値ルールの設定 267

しきい値ルール 267

TelePresence エンドポイント しきい値の設定—デバイス レベル 270

TelePresence エンドポイント しきい値の設定—グローバル 271

会議のトラブルシュートに使用するしきい値の設定 272

TelePresence エンドポイントの自動トラブルシューティングを有効化する 273

デバイス プールのしきい値の概要 273

デバイス プールしきい値の編集 275

音声通話グレード設定の概要 276

Dynamic Syslog の追加 276

相関ルール 279

カスタム アラートの作成 283

カスタム アラートのパラメータ 284

System 286

第 18 章 アラームとイベントのモニタリング 289

アラームとイベントのモニタリング 289

アラームおよびアラーム サマリー 289

[Event] 293

コール イベントの表示 294

アラームとイベントに関する注意事項 295

第 V 部 : ネットワークの監視 299

第 19 章 ビデオ エンドポイントの監視 301

ビデオ エンドポイントの監視 301

エンドポイントの診断ダッシュボード 302

ユーザ詳細の 360° ビューを表示 305

ビデオ テスト コールの管理 307

第 20 章 会議の監視 311

会議の監視 311

ビデオ会議のデータ収集 313

Cisco TMS から会議のインポート 316

会議のワークフローとシナリオ 317

会議の診断ダッシュボード 326

エンドポイントのリアルタイム可視性 331

360° 会議ビュー 334

会議トポロジ 335

エンドポイント統計 338

第 21 章 Cisco APIC-EM を有効にして会議をトラブルシュート 341

Cisco APIC-EM を有効にして会議をトラブルシュート 341

Cisco APIC-EM の概要 341

Cisco APIC-EM コントローラ統合の設定 342

Cisco APIC-EM を使用した会議のトラブルシューティング 343

第 22 章 Cisco Prime Collaboration Assurance サーバの監視 345

Cisco Prime Collaboration Assurance サーバの監視 345

第 VI 部 : ダッシュボードとレポート 351

第 23 章 Cisco Prime Collaboration Assurance ダッシュボード 353

Cisco Prime Collaboration Assurance ダッシュボード 353

Ops View 357

概要（Summary） 364

デバイス プール別のエンドポイント 366

トポロジ - Cisco Unified Communications Manager または Cisco TelePresence Video Communication Server クラスタ 367

接続済みデバイス 372
[パフォーマンス（Performance）] 372
ルート パターンの概要 373
デバイスの検索 373
エンドポイント登録の概要 373
可用性の概要 374
サービス エクスペリエンス/コール品質 375
Top 5 Poor Voice Call Quality Locations 375
Top 5 Call Failure Locations 376
Top 10 TelePresence Endpoints with Call Quality Alarms 377
アラーム付きの会議 377
アラーム ダッシュボード 377
Top 10 TelePresence Endpoints with Alarms 377
Top 10 Devices with Alarms 378
インフラストラクチャ アラームの概要/デバイス アラームの概要 378
使用率モニタ 378
トランク使用率 379
T1/E1 トランク 380
CUBE SIP トランク 381
UCM SIP トランク 383
ルート グループの使用率 384
トランク グループの使用率 385
Location CAC 帯域幅の使用状況 386
会議デバイス 387
Conductor Bridge Pool の使用率 388
TelePresence エンドポイント 389
ライセンスの使用状況（License Usage） 392
カスタマー サマリ ダッシュボード 396
Contact Center Assurance ダッシュボード 398
Contact Center Assurance トポロジ ダッシュボード 399
履歴トレンドの表示 402
Customer Voice Portal（CVP） 403

Unified Contact Center Enterprise（Unified CCE） 413
Cisco Unified Intelligence Center 422
Cisco MediaSense 431
Cisco Unified Contact Center Express 437
Virtualized Voice Browser 442
パフォーマンス ダッシュボード 447
Unified CM と Unity Connection 447
履歴トレンドの表示 462
カスタム パフォーマンス ダッシュボードの作成 464
カスタマイズされたダッシュボードの追加 466

第 24 章 **Cisco Prime Collaboration Assurance レポート** 467
Cisco Prime Collaboration Assurance レポート 467
Cisco Prime Collaboration Assurance レポートを生成するための前提条件 468
CDR データ ソース コール詳細レコード NAM クレデンシャルの更新 468
Prime NAM へのデータ ソースのクレデンシャルの追加 469
複数の Prime NAM クレデンシャルの削除 470
複数の Prime NAM クレデンシャルの確認 470
複数の NAM クレデンシャルの追加 470
Prime NAM クレデンシャルのインポート 472
クレデンシャル検証：エラー メッセージ 472
複数のデータ ソース クレデンシャルの追加 474
NAM クレデンシャルを使用した問題のトラブルシュートとクレデンシャルの確認 475
データ ソース クレデンシャルを使用した問題のトラブルシューティングおよびクレデンシャルの確認 476
コール分類 477
OffNet および OnNetNet コールを理解する 480
コール カテゴリの作成 480
カスタム コール カテゴリの作成 480
ダイヤル プランの追加 481
デフォルトのダイヤル プランを理解する 481
ダイヤル プランにダイヤル パターンを追加 485

ダイヤル プランの編集 488
ダイヤル プランの削除 488
ゲートウェイ コードの設定 488
SFTP 設定項目の設定 489
[SFTP Settings] ページ - フィールドの説明 490
管理レポート 494
CDR および CMR のコール レポート 495
CDR & CMR レポートの生成 504
トラブルシュート 509
NAM & Sensor Report 510
センサー レポートを理解する 516
センサー ストリーム相関データの表示 517
セッション レポート/会議レポート 520
すべてのセッション/会議の要約レポート 521
Session/Conference Detail レポート 522
TelePresence エンドポイント レポート 522
Endpoint Utilization Report 523
No Show エンドポイントの要約レポート 524
[CUCMレポートの起動（Launch CUCM Reports）] 524
その他のレポート 524
UCM/CME Phone Activity Reports 524
Endpoint Move レポート 525
Endpoint Audit レポート 525
Endpoint Remove レポート 525
Endpoint Extension レポート 526
Audio IP Phone Activity レポートの対象期間を理解する 526
Cisco Unified CM がダウン時に電話機のステータスをトラッキング 526
Voice Call Quality Event History Reports 527
その他のレポート 528
CTI Applications レポートの生成 529
ATA Devices レポート 529

Cisco 1040 Sensors レポート 529
会議デバイスのビデオ ポートの使用率レポート 530
スケジュール済みレポート 530
スケジュールされたレポートの生成 533
2,000 件を超えるレコードを含むレポートのデータへのアクセス 533
ファイルのダウンロードに関する問題のトラブルシューティング 534

第 VII 部 : ネットワークの分析 535

第 25 章 Analytics のダッシュボードとレポート 537
Cisco Prime Collaboration Analytics ダッシュボードとレポート 537
Cisco Prime Collaboration Analytics のユーザ役割 538
グローバル顧客の選択 538
グローバル ドメインの選択 538
ユーザ インターフェイス 539
顧客ロゴの管理 543
sFTP サーバの設定 544
Cisco Prime Collaboration Analytics ダッシュレットのデータ入力の前提条件 545
テクノロジー導入 546
エンドポイント モデルによる導入の分配 547
エンドポイント モデルによるコール分配 548
エンドポイント タイプによるコール分配 549
テクノロジーの使用 550
資産使用状況 551
使用頻度が最も低いエンドポイント タイプ 551
ビデオ テレプレゼンス ルームの使用率 552
No Show Video TelePresence エンドポイント 552
トラフィック分析 554
上位 N の発信者 554
上位 N のダイヤル番号 555
上位 N のオフネット トラフィック拠点 555

上位 N コール トラフィック拠点 556
コール トラフィック分析 557
キャパシティ分析 558
分析グループの管理 558
CAC 帯域幅使用率 559
トランク使用率 560
煩雑時のトランク キャパシティ 560
ルート グループ/トランク グループの使用率 563
煩雑時のルートグループ キャパシティ 563
DSP 使用率 565
サービス エクスペリエンス 565
サービス エクスペリエンスの分配 566
サービス品質問題があるエンドポイント 568
上位 N のコール失敗発生拠点 569
サービス品質問題があるユーザ 570
Call Grade for Locations 571
ビデオ会議 571
ビデオ会議の統計情報 572
上位 N のビデオ会議の拠点 573
会議用デバイスのビデオ使用率 574
Conductor Bridge Pool の使用率 574
UC システム パフォーマンス 575
ライセンスの使用状況（License Usage） 576
Contact Center Enterprise 576
顧客音声ポータル 576
マイ ダッシュボード 578
カスタム レポート 578
カスタム レポートの作成 580
スケジュール済みレポート 580
Prime Collaboration Analytics ダッシュボードのトラブルシューティング 582

第 VIII 部： 診断の実行 585

第 26 章 音声エンドポイントの診断 587

音声エンドポイントの診断 587

Phone Status Test 587

Phone Status Test の作成 588

Phone Status Test のインポート 589

Synthetic Test 592

Synthetic Test の前提条件 594

Emergency Call Synthetic Test の作成 595

Synthetic Test メッセージ待機インジケータの作成 596

TFTP Download Synthetic Test の作成 597

HTTP Download Synthetic Test の作成 598

End-to-End Call Synthetic Test の作成 598

Dial-Tone Synthetic Test の作成 600

Phone Registration Test の作成 601

Synthetic Test のインポート 602

Synthetic Test の管理 608

模擬テストに関する特記事項 609

IP SLA 音声テスト 611

Cisco IOS および IP SLA の必要なバージョン 615

[IP SLA音声テスト（IP SLA Voice Test）] を作成します。 615

[複数をインポート（Import Multiple）][IP SLA音声テスト（IP SLA Voice Tests）] 621

[IP SLA音声テスト（IP SLA Voice Tests）] の管理 624

IP SLA 音声テスト データ 626

バッチ テストの作成 635

バッチ テスト インポート ファイルの形式 635

Batch Test の管理 637

Phone Test：Batch および On Demand Test 640

Phone Test on Demand の作成 642

Audio Phone Features Test 644
トラブルシューティング 653
CME 診断 654
Cisco Unified CME Syslog メッセージを使用した IP フォンの監視 655

第 27 章 ビデオ エンドポイントのトラブルシューティング ワークフロー 657
ビデオ エンドポイントのトラブルシューティング ワークフロー 657
トラブルシューティング ワークフローの機能 659
会議のトラブルシューティング ワークフローの機能 660
エンドポイントのトラブルシューティング ワークフローの機能 661
発信元と宛先のエンドポイントをトラブルシューティングするためのサポート マトリクス 662
トラブルシューティング ワークフローの開始 664
データ分析のトラブルシュート 666
トラブルシューティング 666
パス統計 672
トラブルシューティング データのエクスポート 675
トラブルシューティング レポートのエクスポートを理解する 676
Cisco Prime Infrastructure のクロス起動 678
Cisco Prime Infrastructure のクロス起動 679

第 28 章 メディア パスの分析 681
メディア パスの分析 681
VSAA を使用したメディア パスの分析 681
VSA エージェントの検査結果 682

第 29 章 ログの収集 685
ログの収集 685
ログ収集センター/デバイス ログ コレクター 686
トレース レベルの設定 689
ログ収集テンプレート 690

コール ログの収集 690

第 30 章 コール シグナリングの分析 693

コール シグナリングの分析 693

サポートされるコール フロー 696

コール ラダー ダイアグラムの作成 697

コール ラダー ダイアグラムのメッセージのフィルタリング 700

コール ラダー ダイアグラムについて 700

第 IX 部 : サーバの保守 703

第 31 章 ジョブの管理 705

ジョブの管理 705

ジョブをスケジュールする 707

タイムテーブルの定義 709

ジョブのキャンセル 710

事前定義済みのクイック フィルタ 710

第 32 章 パージ ポリシー 713

パージ ポリシー 713

パージ ポリシー テーブル 713

第 33 章 バックアップと復元の実行 717

バックアップと復元の実行 717

バックアップと復元の概要 717

バックアップ期間 718

FTP、ディスク、SFTP、または TFTP サーバでのリポジトリの作成 719

Cisco Prime Collaboration Assurance および Analytics ユーザ インターフェイスを使用したスケジュールのバックアップ 720

トラブルシューティング 723

CLI を使用した Cisco Prime Collaboration Assurance データのバックアップ 723

バックアップ履歴の確認 724
同じシステムでのデータの復元 724
新しいシステムでの復元 724

第 34 章 ログ レベルの設定 725
ログ レベルの設定 725
ログ レベル 725

第 X 部 : Unified Communication Operations ダッシュボード 727

第 35 章 Unified Communication Operations ダッシュボードの概要 729
Unified Communication Operations ダッシュボード 729
Unified Communication Operations Dashboard の概要 729
PCA へのレスポンダのインストール 729
UC 運用ダッシュボードの起動 730
マスター IP アドレスの登録 730
Unified Communication Operations のランディングページ 731

第 36 章 しきい値設定 733
しきい値設定の概要 733
しきい値設定 733
しきい値パラメータ 734

第 37 章 システム設定 735
システム設定 735
関連付けられたレスポンダの追加または削除 735
ジョブ頻度の設定 737
共有秘密キーの設定 737

第 38 章 レスポンダ設定 739
レスポンダ設定の概要 739

レスポンダの有効化 739
共有秘密キーの設定 739
登録ステータス 740

第 章 参考資料 741

付録 A： Synthetic Test ワークシート 743
Synthetic Test ワークシート 743

付録 B： Cisco 1040 センサー管理 747
Cisco 1040 センサー管理 747
Cisco Prime NAM/vNAM の概要 747
Cisco Prime Collaboration Assurance の初期設定を実行 748
Cisco 1040 設定およびイメージ ファイル用の TFTP サーバの設定 748
TFTP サーバの追加と削除 748
Cisco 1040 センサー デフォルト設定のセットアップ 749
Cisco Prime Collaboration Assurance で Cisco 1040 センサーを設定 751
Cisco 1040 センサーの詳細 751
Cisco 1040 センサーの追加 753
複数の Cisco 1040 設定を編集 754
Cisco 1040 管理：フィールドの説明 755
Cisco 1040 のリセット 755
Cisco 1040 センサーの削除 756
Cisco 1040 の診断情報を表示 757

付録 C： セキュアな JTAPI 接続のトラブルシューティング 759
セキュアな JTAPI 接続のトラブルシューティング 759

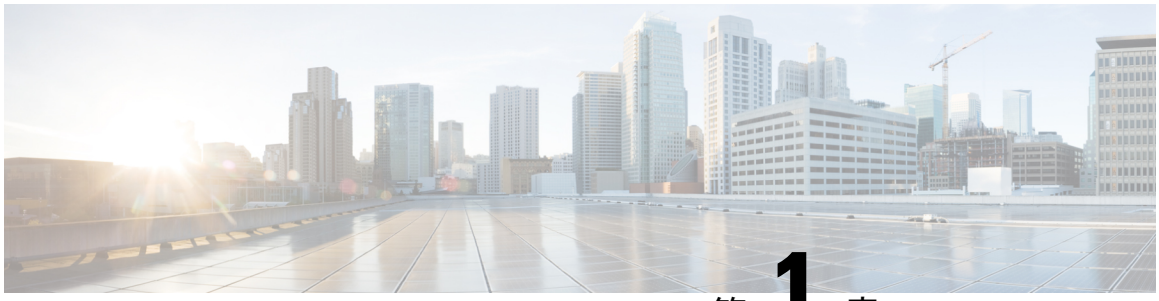
付録 D： Jetty および Tomcat サーバの TLS 設定 761
Cisco Prime Collaboration Assurance のクライアント接続で最小 TLS バージョンの有効化 761
Jetty サーバで TLS プロトコルの有効化 762
Tomcat サーバで TLS プロトコルの有効化 762

付録 E： ユーザ インターフェイス 765
概要 765
フィルタ（Filters） 767
拡張フィルタの開始とフィルタ基準の保存 768
クイック ビュー 768
製品情報の詳細の表示 768

第 I 部

Cisco Prime Collaboration の開始

- Cisco Prime Collaboration Assurance および Analytics の概要 （1 ページ）
- 概要 （43 ページ）
- Cisco Prime Collaboration Assurance を開始する （51 ページ）



第 1 章

Cisco Prime Collaboration Assurance および Analytics の概要

このセクションでは、Cisco Prime Collaboration Assurance および Analytics の概要について説明します。

- Cisco Prime Collaboration Assurance の概要 （1 ページ）
- Cisco Prime Collaboration Assurance の概要 - MSP モード （19 ページ）
- Enterprise モードと MSP モードの違い （24 ページ）
- Cisco Prime Collaboration Assurance NBI （26 ページ）
- Cisco Prime Collaboration Assurance および Analytics の Geo-Redundancy （27 ページ）
- 新機能および変更された機能に関する情報, on page 27
- Cisco Prime Collaboration Assurance の新機能, on page 30
- Cisco Prime Collaboration Analytics の概要 （39 ページ）

Cisco Prime Collaboration Assurance の概要

このドキュメントでは、Cisco Prime Collaboration Assurance 11.0、11.1、11.5、11.6、12.1、12.1 SP1 の機能について説明します。

Cisco Prime Collaboration Assurance は、モニタリング、、レポート機能を備えた包括的なビデオおよび音声サービスのアシュアランスおよび管理システムで、ユーザに一貫した高品質のビデオおよび音声コラボレーション体験を提供します。

表記法

次の規則が、Cisco Prime Collaboration Assurance のさまざまなリリース用のドキュメントで使用されています。

- すべての関連セクションでは、「セッション」から「会議」へと名前変更されました。

（注） 「セッション」という用語は、Cisco Prime Collaboration Assurance Release 11.1 以前のバージョンに適用されます。

- すべての関連セクションでは、「[Log Collection Center]」 から 「[Device Log Collector]」へと名前変更されました。

（注） 「[ログ収集センター（Log Collection Center）]」 という用語は、Cisco Prime Collaboration Assurance Release 11.1 以前に適用されます。

- すべての関連セクションでは、「[Call Signalling Analyzer]」 から 「[SIP Call Flow Analyzer]」へと名前変更されました。

（注） 「[コール シグナリングの分析（Call Signaling Analyzer）]」 という用語は、Cisco Prime Collaboration Assurance Release 11.1 以前に適用されます。

- Cisco Prime Collaboration Assurance Release 11.5 では、「トラブルシューティング」 はサポートされていません。

（注） 「トラブルシューティング」は、Cisco Prime Collaboration Assurance Release 11.1 以前に適用されます。

- **[Limited Visibility]** オプションは、Cisco Prime Collaboration Assurance 12.1 以降のダッシュボードではサポートされていません。**[Edit Visibility]** をクリックして、**[Full Visibilty]** オプションまたは [OFF] に切り替えます。
- 「FIPS コンプライアンス」は Cisco Prime Collaboration Assurance Release 12.1 でサポートされていません。

（注） 「FIPS コンプライアンス」は、Cisco Prime Collaboration Assurance Release 11.6 以前に適用されます。

- 「クレデンシャル プロファイル」機能は、Cisco Prime Collaboration Assurance Release 11.6 の MSP モードでサポートされません。

（注） これにより、TelePresence エンドポイントは [アクセス（不可 Inaccessible）] として表示されます。

- 「スマート ライセンシング」 機能は、Cisco Prime Collaboration Assurance リリース 12.1 でサポートされません。
- Mobile and Remote Access（MRA）ソリューションを使用してエンドポイントが登録されている場合、「ビデオ テスト コール」機能はサポートされません。
- SSL が有効な LDAP 設定は、Cisco Prime Collaboration Assurance Release 12.1 でサポートされません。
- ユーザ インターフェイスに [CUCM SFTP クレデンシャル（CUCM SFTP Credentials）] や [保存（Save）] などのタブが追加されました。同じユーザのパスワードを変更するためのフィールドと、パスワードオプションを確認するためのオプションを使用できます。Cisco Prime Collaboration Assurance Release 12.1 Service Pack 3 では、ナビゲーションが **[アラームとレポート管理（Alarm & Report Administration）]** -> **[CDR ソース設定（CDR Source Settings）]** -> **[CUCM SFTP クレデンシャル（CUCM SFTP Credentials）]** から **[インベントリ（Inventory）]** -> **[インベントリ管理（Inventory Management）]** -> **[CUCM SFTP クレデンシャル（CUCM SFTP Credentials）]** へと変更されました。
- Release 12.1 Service Pack 3 の Cisco Prime Collaboration Assurance ユーザ インターフェイスから、[CDR Source Settings] ダッシュレットと [Manage Call Quality Data Source Settings] ページが削除されました。

Cisco Prime Collaboration Assurance - Advanced

Cisco Prime Collaboration Assurance は次のモードで利用できます。

- Cisco Prime Collaboration Assurance Advanced：Enterprise モードと MSP モード

および Advanced Assurance のインストールについては、『Cisco Prime Collaboration Assurance および Analytics のインストールとアップグレード ガイド』を参照してください。

Cisco Prime Collaboration Assurance Advanced は、ユーザが一貫した高品質のビデオおよび音声コラボレーションエクスペリエンスを確実に受信できるようにするモニタリング、、およびレポート機能を備えた包括的なビデオおよび音声サービス保証および管理システムです。

- Enterprise モードは、企業内で 1 つのエンタープライズ ビューまたは複数のドメイン ビューを提供します。このオプションは通常、標準のシングルエンタープライズ環境で使用されます。
- MSP モードは複数のカスタマー ビューを提供します。このオプションは、マネージドサービス プロバイダーの環境で使用します。このビューでは、管理されている複数のカスタマーのデバイスを表示できます。MSP モードの詳細については、『Cisco Prime Collaboration Assurance ガイド - Advanced』の*Cisco Prime Collaboration Assurance* の概要 — *MSP* モード」を参照してください。

次の表には、Cisco Prime Collaboration Assurance - および Advanced で利用可能な機能が示されています。

機能	Advanced	『Cisco Prime Collaboration Assurance ガイド - Advanced』の参照先
サポート対象モード	Enterprise モードと MSP モードをサポートしています。	Advanced の機能の詳細については、「*Overview of Cisco Prime Collaboration Assurance—MSP Mode*」および「*Differences Between the Enterprise Mode and the MSP Mode*」の項を参照してください。
ライセンス要件	評価期限が切れると、ライセンスが必要になります。	Advanced の機能の詳細については、「*Manage Licenses*」の項を参照してください。
ロール ベース アクセス コントロール	5つのロールをサポートして複数の承認レベルを提供します。 • スーパー管理者 • システム管理者 • ネットワーク管理者 • オペレータ • ヘルプデスク **Cisco Prime Collaboration リリース 11.5 以降の場合** 6つのロールをサポートして複数の承認レベルを提供します。 • スーパー管理者 • システム管理者 • ネットワーク管理者 • オペレータ • ヘルプデスク • レポート ビューア	Advanced の機能の詳細については、「*Manage Users*」の項を参照してください。
シングル サインオンのサポート	対応	Advanced の機能の詳細については、「*Manage Users*」の項を参照してください。
クラスタの管理	クラスタのリビジョンとクラスタの関連付けが混在する複数のクラスタを管理します。	Advanced の機能の詳細については、「*Set Up Clusters*」の項を参照してください。

検出	• Cisco Unified CM（電話機および TelePresence）、Cisco VCS（TelePresence）、Cisco TMS（TelePresence）に登録されているすべてのエンドポイントを検出し、管理することができ ます。エンドポイントの管理に加えて、音声およびビデオ コラボレーション ネットワークに含まれる、マルチポイント スイッチ、アプリケーション マネージャ、コール プロセッサ、ルータ、スイッチも管理できます。 • 自動検出、インポート、デバイス追加の機能などの複数の検出モードを提供します。 • デバイスを検出するために、論理検出、ping スウィープ、CDP ベースの検出をサポートします。 • 再検出を実行するためのオプションを提供します。 **Cisco Prime Collaboration リリース 11.5 以降の場合** （注） CTS-Manager（TelePresence）デバイスはサポートされていません。	Advanced の機能の詳細については、「*Discover Devices*」の項を参照してください。
インベントリ管理	• デバイス 360° ビューから、デバイスの簡潔な概要情報を提供します。 • 包括的なインベントリ詳細を提供します。	Advanced の機能の詳細については、「*Manage Inventory*」の項を参照してください。

障害管理	• **Cisco Prime Collaboration リリース 11.1 以前の場合**
	クイック ビューを使用したトラブルシューティングの開始をサポートします。
	• アラーム相関ルールをサポートします。
	• デバイスおよびグローバル レベルでのイベントのカスタマイズをサポートします。
	• 次のしきい値の設定を行います。
	  • TelePresence エンドポイント
	  • インフラストラクチャ デバイス
	  • コール品質
	  • デバイス プール
		Advanced の機能の詳細については、「*Monitor Alarms and Events*」の項を参照してください。

音声およびビデオ レポート	次の定義済みレポートとカスタマイズ可能なレポートを提供します。 • 管理レポート • Communications Manager のレポート • インタラクティブ レポート • スケジュール設定されたレポート	Advanced の機能の詳細については、「*Dashboards and Reports*」の項を参照してください。

ダッシュボード	次のダッシュボードを提供します。 • [Ops View]：Cisco Unified CM および VCS クラスタの概要を提供します。 • サービス エクスペリエンス - サービス品質に関する情報を提供します。 • アラーム - アラームの概要に関する情報を提供します。 • [Performance]：各管理対象デバイスの重要なパフォーマンス メトリックについて詳細情報を提供します。 • Contact Center トポロジ - CUIC、Finesse、MediaSense、CVP、Unified CCE など、Contact Center のコンポーネントに関する情報を提供します。 ホーム ページに、カスタマイズされたダッシュボードを追加できます。	Advanced の機能の詳細については、「*Dashboards and Reports*」の項を参照してください。

ダッシュボード	**Cisco Prime Collaboration リリース 11.5 以降の場合** 次のダッシュボードを提供します。 • • [Ops View]：Cisco Unified CM および VCS クラスタの概要を提供します。 • コール品質 - サービス品質に関する情報を提供します。 • アラーム - アラームの概要に関する情報を提供します。 • [Performance]：各管理対象デバイスの重要なパフォーマンス メトリックについて詳細情報を提供します。 • Contact Center トポロジ - CUIC、Finesse、MediaSense、CVP、Unified CCE など、Contact Center のコンポーネントに関する情報を提供します。 ホーム ページに、カスタマイズされたダッシュボードを追加できます。 また、次の操作を実行できます。 • 既存のダッシュレットを別のダッシュボードに追加します。 • ダッシュレットをドラッグアンドドロップして、ダッシュボードの下に移動します。	Advanced の機能の詳細については、「*Dashboards and Reports*」の項を参照してください。

音声およびビデオ エンドポイントの診断	**Cisco Prime Collaboration リリース 11.1 以前の場合** • エンドポイント、サービス インフラストラクチャ、およびネットワーク関連問題の具体的な情報など、エンドツーエンド メディア パスを詳細に分析します。 • ビデオの問題を特定するために Cisco メディアネット テクノロジーを使用します。 • メディア パス計算、統計収集、合成トラフィックの生成を行います。 • IP SLA を使用して、ネットワーク内の主要な IP フォンの応答可能性を監視します。 • スケジュールした合成および IP SLA テストを使用して、サービスの停止を予測します。 **Cisco Prime Collaboration リリース 11.5 以降の場合** • IP SLA を使用して、ネットワーク内の主要な IP フォンの応答可能性を監視します。 • スケジュールした合成および IP SLA テストを使用して、サービスの停止を予測します。	Advanced の機能の詳細については、「*Perform Diagnostics*」の項を参照してください。
ジョブ管理	ユーザがジョブを表示、スケジュール、および削除できるようにします。	Advanced の機能の詳細については、「*Manage Jobs*」の項を参照してください。
UC アプリケーションの相互起動	Yes	-

Cisco Prime Collaboration Assurance サービスアビリティへのクロス起動	Yes	-
デバイスの検索	グローバル検索：TelePresence、エンドポイント、電話、その他のデバイス、場所、およびユーザに対してフィルタ処理された検索を提供します。	Advanced の機能の詳細については、「*Global Search Options for Cisco Prime Collaboration Assurance*」の項を参照してください。

Cisco Prime Collaboration Analytics	ネットワーク内のトラフィックの傾向、テクノロジーの導入傾向、過度に使用されているリソース、あまり使用されていないリソースを簡単に特定できるようにします。また、断続的に発生したり、繰り返し発生したりするネットワークの問題を追跡し、Analysticsのダッシュボードを使用してサービス品質の問題に対処できます。Analisticsのダッシュボードには以下が含まれます。 • テクノロジー導入 • 資産使用状況 • トラフィック分析 • キャパシティ分析 • コール品質 • UC システム パフォーマンス • スケジュール設定されたレポート • ビデオ会議 • カスタム レポート ジェネレータ （注） **Cisco Prime Collaboration リリース 11.1 以前の場合** Cisco Prime Collaboration Analytics は MSP モードの導入ではサポートされません。 Cisco Prime Collaboration Analytics は、ライセンスを必要とするソフトウェアで、Cisco Prime Collaboration Assurance とは別に購入する必要があります。	『Cisco Prime Collaboration Analytics Guide』を参照してください。

NB API	NB API は、次の場合にサポートされます: • デバイスの管理 • デバイス クレデンシャルの表示および削除 • すべてのビデオ会議を一覧表示 • **Cisco Prime Collaboration リリース 11.1 以前の場合** ビデオ会議のトラブルシューティング	NB API のドキュメントにアクセスするには、管理者権限で Cisco Prime Collaboration Assurance サーバにログインし、ブラウザの URL に http://<pc-server-ip>/emsam/nbi/nbiDocumentation を入力します。 ここで、pc-server-ip は Cisco Prime Collaboration Assurance サーバの IP アドレスです。 **Cisco Prime Collaboration リリース 11.6 以降の場合** NB API ドキュメントにアクセスするには、Cisco Prime Collaboration Assurance サーバにログインし、ユーザインターフェイスの右上隅にある [設定（Settings）] のドロップダウン メニューから **[Assurance NB API ドキュメント（Assurance NB API documentation）]** を選択します。

Cisco Prime Collaboration Assurance - Advanced 機能

Cisco Prime Collaboration Assurance ではネットワークを監視し、診断を実行することができます。また、問題の原因の特定に役立つレポートを実行できます。

音声とビデオの Unified Dashboard

Cisco Prime Collaboration Assurance ダッシュボードでは、音声およびビデオ コラボレーション ネットワークのエンド ツー エンドでの監視が可能になります。次の概要が提供されます。

ダッシュボード	説明	Cisco Prime Collaboration Assurance オプション
サービス エクスペリエンス	やサービス品質に関する情報です。	Cisco Prime Collaboration Assurance Advanced
アラーム	に関する情報です。アラームの概要です。	Cisco Prime Collaboration Assurance
パフォーマンス	各管理対象デバイスの重要なパフォーマンス メトリックについて詳細情報を提供します。	Cisco Prime Collaboration Assurance Advanced

Contact Center トポロジ	に関する情報です。Unified Contact Center のトポロジ ビューです。	Cisco Prime Collaboration Contact Center Assurance

Cisco Prime Collaboration リリース 11.5 以降の場合

ダッシュボード	説明	Cisco Prime Collaboration Assurance オプション
コール品質	サービス品質に関する情報です。	Cisco Prime Collaboration Assurance Advanced
アラーム	アラームの概要に関する情報です。	Cisco Prime Collaboration Assurance
パフォーマンス	各管理対象デバイスの重要なパフォーマンス メトリックについて詳細情報を提供します。	Cisco Prime Collaboration Assurance Advanced
Contact Center トポロジ	に関する情報です。Unified Contact Center のトポロジ ビューです。	Cisco Prime Collaboration Contact Center Assurance

Cisco Prime Collaboration Assurance サーバの導入後にダッシュレットを追加する方法については、「「Prime Collaboration ダッシュボード」」を参照してください。

[デバイスインベントリ（DeviceInventory）]/[インベントリ管理（InventoryManagement）]

Cisco Unified Communications Manager（電話と TelePresence）、Cisco Expressway（TelePresence）、および Cisco TMS（TelePresence）に登録されたすべてのエンドポイントを検出、管理できます。エンドポイントの管理に加えて、音声およびビデオ コラボレーション ネットワークに含まれる、マルチポイント スイッチ、アプリケーション マネージャ、コール プロセッサ、ルータ、スイッチも管理できます。

検出では、デバイス インターフェイスと周辺機器の詳細も取得され、Cisco Prime Collaboration Assurance に保存されます。

検出が完了したら、次のデバイス管理タスクを実行できます。

- デバイスをユーザ定義グループにグループ化します。
- 管理対象デバイスの可視性の設定を編集します。
- デバイスのイベント設定をカスタマイズします。
- デバイスを再検出します。
- 管理対象デバイスのインベントリを更新します。
- 管理対象デバイスの管理を一時停止およびレジュームします。
- グループからデバイスを追加または削除します。

- デバイス クレデンシャルを管理します。
- デバイスの詳細をエクスポートします。

エンドポイント インベントリ データの収集方法とその管理方法については、「インベントリの管理」を参照してください。

音声およびビデオのエンドポイント モニタリング

サービス オペレータは、企業内のすべての音声とビデオ 会議のネットワークでサービスの劣化が生じた場合は、原因を迅速に切り分ける必要があります。

Cisco Prime Collaboration リリース 11.1 以前の場合

Cisco Prime Collaboration Assurance は、エンドポイントのスペック、サービス インフラストラクチャ、ネットワーク関連の問題などエンド ツー エンドのメディアパスの詳細分析を提供します。

ビデオ エンドポイントでは、Cisco Prime Collaboration Assurance により、すべての [Point-to-point（ポイント ツー ポイント）]、[Multisite（マルチサイト）]、[Multipoint（マルチポイント）] によるビデオ コラボレーション 会議を監視することができます。これらの会議は、次のいずれかのステータスとともにアドホック、スタティック、またはスケジュール済みとなります。

- In-progress
- Scheduled
- Completed
- No Show

Cisco Prime Collaboration Assurance は、次の場所から情報を定期的にインポートします。

- スケジュール済みの会議での管理アプリケーション（および Cisco TMS）や会議デバイス（CTMS、Cisco MCU、Cisco TS）。
- エンドポイントの登録時やコール ステータスに表示される、コールや会議のコントロール デバイス (Cisco Unified CM および Cisco Expressway）。

また、Cisco Prime Collaboration Assurance は、Cisco Collaboration システムがサポートするアクティブ コールを継続的に監視し、コールの音声品質がユーザ定義の品質しきい値を満たさない場合は、ほぼリアルタイムに通知を提供します。Cisco Prime Collaboration Assurance では、ローカル ダイヤルプランに基づきコールを分類することもできます。

IP フォンや TelePresence の監視方法を理解するには、Cisco Prime Collaboration のネットワーク監視、レポーティング、診断ガイド、9.x 以降の「監視用ネットワークをセットアップするための前提条件」を参照してください。

診断

Cisco Prime Collaboration Assurance は、Cisco Medianet テクノロジーを使用して、ビデオに関する問題を特定および分離します。メディア パス計算、統計情報収集、および合成トラフィックの生成を行います。

ネットワーク デバイスが Medianet に対応している場合、Cisco Prime Collaboration Assurance は次のものを提供します。

- Mediatrace を使用したビデオ パスに沿ったフロー関連情報。
- Performance Monitor を使用した、ネットワーク ホット スポットでのすべてのトラフィックのスナップショット ビュー。
- ネットワーク上のビデオ パフォーマンスを評価するために、IP サービスレベル契約（IP-SLA）とビデオ サービスレベル契約（VSAA）を使用して、ネットワーク デバイスから合成ビデオ トラフィックを開始する機能。

IP 電話では、Cisco Prime Collaboration Assurance は IP SLA を使用して、ネットワーク内の主要電話の応答可能性を監視します。電話ステータス テストは、次の内容で構成されます。

- テスト対象 IP フォンのリスト。
- 設定可能なテストのスケジュール。
- IP フォンに対して IP SLA 対応デバイス（スイッチ、ルータ、または音声ルータなど）から IP SLA ベースの ping。オプションとして、Cisco Prime Collaboration Assurance サーバから IP 電話に ping することもできます。

Cisco Prime Collaboration リリース 11.5 以降の場合

Cisco Medianet テクノロジーはサポートされていません。

Cisco Prime Collaboration Assurance を使用すると、コール ログを収集して、Cisco Voice Portal（CVP）、Unified Contact Center Enterprise（Unified CCE）、Cisco Unified Communications Manager（Unified CM）、および IOS ゲートウェイへのコールの障害を特定できます。この機能により、コールの問題のトラブルシューティングができます。SIP Call Flow Analyzer 機能を使用し、収集したコールをさらに詳しく調べて、メッセージ内の問題点を特定することができます。また、コールメッセージに障害があることを示すコール ラダーダイアグラムを表示して、根本的な原因と推奨事項を提供できるため、問題の再現にも役立ちます。

障害管理

Cisco Prime Collaboration Assurance によって、ほぼリアルタイムで迅速かつ的確な障害検出が行われます。Cisco Prime Collaboration Assurance は、イベントの特定後に、イベントを関連するイベントでグループ化し、障害分析を実行して障害の根本原因を判別します。

Cisco Prime Collaboration Assurance では、個々のユーザにとって重要なイベントをモニタリングできます。また、イベントの重大度をカスタマイズできるほか、その重大度に基づいてCisco Prime Collaboration Assurance から通知を受け取ることもできます。

Cisco Prime Collaboration Assurance は、アラームとイベントに関するトラップを生成し、トラップの受信者に通知を送信します。これらのトラップは、Cisco Prime Collaboration Assurance サーバによって生成されたイベントとアラームに基づきます。トラップは SNMPv2c 通知に変換され、CISCO-EPM-NOTIFICATION-MIB に従ってフォーマットされます。

Cisco Prime Collaboration Assurance での障害モニタリングについては、「アラームとイベントのモニタリング」を参照してください

レポート

Cisco Prime Collaboration Assurance は、次の定義済みおよびカスタマイズ可能なレポートを提供します。

- Administrative レポート — Provides System Status レポート、Who Is Logged On レポート、プロセス ステータスを提供します。
- CDR & CMR レポート — コール カテゴリ タイプ、コール クラス、コール時間、終了タイプ、コール リリース コードなど、コールの詳細を提供します。
- Conference レポート — All Conference Summary レポートと Conference Detail レポートを提供します。
- TelePresence Endpoint レポート — 完了済みおよび進行中の会議、エンドポイントの使用率、No Show エンドポイントの詳細を提供します。TelePresence レポートには、会議デバイスの一覧や、ネットワーク内の平均およびピーク使用率も提供されます。
- Launch CUCM レポート — Cisco Unified Communications Manager クラスタのレポートページへとクロス起動できるようにします。
- Miscellaneous レポート — UCM/CME Phone Activity レポート、Voice Call Quality Event History レポートなど、さまざまなレポートを提供します。
- Scheduled レポート — 使用率およびインベントリ レポートを提供します。レポートは、その場で生成するか、スケジューリングを有効にして事前に定義された日に生成できます。

さまざまなレポートのタイプとその生成方法については、Cisco Prime Collaboration Assurance レポート を参照してください。

IPv6 用の Cisco Prime Collaboration Assurance サポート

Cisco Prime Collaboration Assurance は、IPv6 のみの IPv6 エンドポイントとデュアル スタック ネットワークをサポートします。次の表には、IPv6 エンドポイントをサポートする Cisco Prime Collaboration Assurance 機能の詳細が示されています。

表 *1 : IPv6* デバイスをサポートする *Cisco Prime Collaboration Assurance* 機能

機能	サポートあり	注釈または制限
デバイスインベントリ/インベントリ：クレデンシャル プロファイル	IPv6 クレデンシャル プロファイルの作成	—
デバイスインベントリ/インベントリ：検出	• IPv6 クレデンシャル プロファイルを承認して、これらのプロファイルを IPv6 アドレスに一致させることができる • Ping して iPv6 デバイスに到達する • エンドポイントが IPv4、IPv6、デュアル スタックを使用して Unified CM に登録されている場合は、アクティブな IP アドレス（登録したエンドポイントと通信するため Unified CM 設定で選択した IP アドレス）のみが表示されます。 • エンドポイントが ならびに IPv4、IPv6、またはデュアル スタックを介して VCS に登録することができる場合、VCS に登録したデバイスの IP アドレスを確認できます。	• Unified CM、TMS、CTS、その他のインフラストラクチャ デバイスは、IPv4 を使用した場合のみ管理できます。 • Ping スイープ検索は、IPv6 サブネット上では機能しません。
デバイスインベントリ/インベントリ：インベントリ管理	インベントリ概要には IPv6 アドレスが表示されます。	—
会議の診断	エンドポイント統計（システムと会議情報）には IPv6 アドレスが表示されます。 エンドポイントのクイック ビューには IPv6 アドレスが表示されます。	—

機能	サポートあり	注釈または制限
エンドポイントの診断	エンドポイントの診断ダッシュボードには IPv6 アドレスが表示されます。	—
トラブルシューティング	—	IPv6 デバイスではトラブルシューティングをサポートしていません。
ダッシュボードとレポート	その他のレポート：Voice Call Quality Event History レポートと UCM/CME Phone Activity レポートには IPv6 アドレスが表示されます。	デフォルトでは、IPv6 アドレス列は非表示になっています。[列フィルタ（Column Filter）] アイコンをクリックすると、表示する列を変更できます。
トポロジ	IPv6 アドレスを持つエンドポイントを検索します。	—
Alarm ブラウザ	アラーム概要には、IPv6 アドレスが表示されます。	—
電話機の検索	IPv6 フォンを検索します。	—
Cisco Prime Collaboration リリース 11.5 以降の場合		
テクノロジ導入ダッシュボード	IP アドレス フィルタは、IPv6 アドレスを持つエンドポイントをサポートします。	—
資産使用状況ダッシュボード	IP アドレス フィルタは、IPv6 アドレスを持つエンドポイントをサポートします。	—
トラフィック分析ダッシュボード	IP アドレス フィルタは、IPv6 アドレスを持つエンドポイントをサポートします。	—
サービス体験ダッシュボード	IP アドレス フィルタは、IPv6 アドレスを持つエンドポイントをサポートします。	—

（注）
- デュアル スタック デバイスの場合、前述の IP アドレス列には、UCM/UCE のおよび Phone Activity レポートを除き、IPV4 IP アドレスのみが表示されます。
- North Bound Interface（NBI）通信は、IPv4 ネットワークのみでサポートされています。
- コロン（:）は、クレデンシャル プロファイル パターンのセパレータとして、または複数のデバイスを追加するときには使用できません。

Cisco Prime Collaboration Assurance の概要 - MSP モード

Cisco Prime Collaboration Assurance の MSP モードでは複数のカスタマー ビューを提供します。このオプションは、マネージド サービス プロバイダーの環境で使用します。カスタマーごとに制限されたアクセスを実装し、管理を独立させることによって、複数のカスタマーのネットワーク（スタティック NAT 環境など）をより高度に管理することができます。

（注） MSP モードの導入を選択できるのはインストール中のみです。

NAT 環境 - 導入シナリオ

次のシナリオで、NAT の背後にあるカスタマーのエンドポイントを管理できます。

- シナリオ - 音声エンドポイント

  NAT 環境で Call Controller （エンドポイントのプライベート IP アドレスで設定）に登録済みの音声電話機 - Cisco Prime Collaboration Assurance ではパブリック IP アドレス（別称は管理対象 IP アドレス）で管理されています。

- シナリオ - 音声およびビデオ エンドポイント

  NAT 環境のカスタマー プレミス内にある Call Controller に登録済みの音声およびビデオ/TelePresence エンドポイント - Cisco Prime Collaboration Assurance ではパブリック IP アドレス（別称は管理対象 IP アドレス）で管理されています。

- **Cisco Prime Collaboration リリース 11.1 以前の場合**

  シナリオ - TelePresence が Cisco TelePresence Exchange（CTX）にプロビジョニングされている

  NAT 環境で CTX にプロビジョニングされている TelePresence エンドポイント - Cisco Prime Collaboration Assurance ではパブリック IP アドレス（別称は管理対象 IP アドレス）で管理されています。

（注） コール マネージャ上で Cisco Unified Communications Manager が処理するノード（UCM クラスタのパブリッシャ）のクエリが、パブリッシャの IP アドレスまたはホスト名を返します。NAT 環境では、パブリッシャークエリ出力として返されるパブリックホスト名は、Cisco Prime Collaboration Assurance のプライベート DNS 設定で解決しないようにする必要があります。

たとえば、パブリック ホスト名が FQDN の場合、プライベート DNS は FQDN のないホスト名であるか、異なる FQDN のホスト名、すなわちパブリック ドメインである必要があります。

（注） **Cisco Prime Collaboration リリース 11.5 以降の場合**

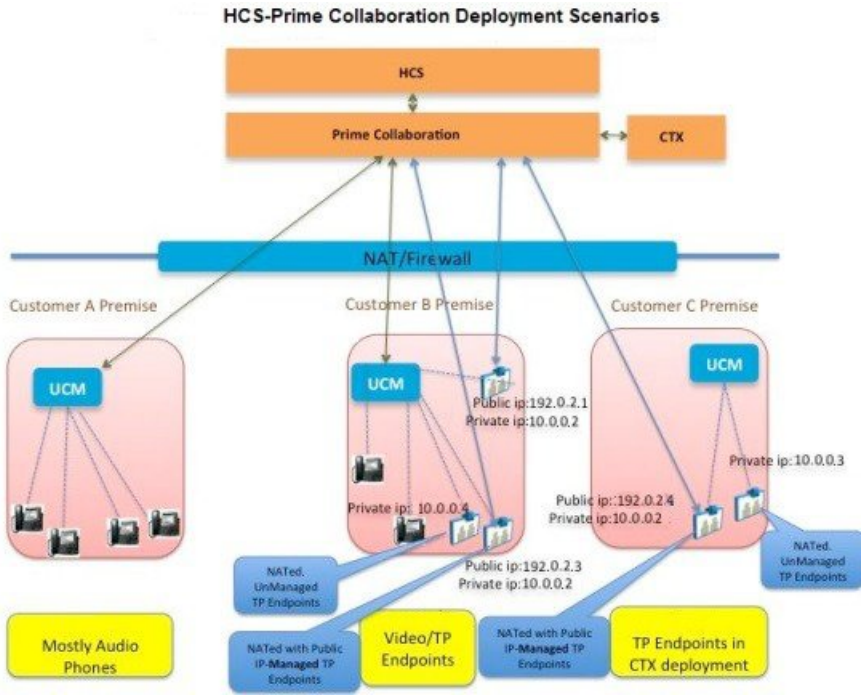
1 人のお客様が使用するデバイスのプライベート IP アドレスは、別のお客様が使用するデバイスのパブリック IP アドレスと重複する場合があります。ただし、パブリック IP アドレスは、Cisco Prime Collaboration Assurance が管理するお客様の間ではそれぞれが異なります。

たとえば、「顧客 A」 の IP フォンのプライベート IP アドレス（192.168.1.12）が、「顧客 B」の Unified Communications Manager のパブリック IP アドレス（192.168.1.12）と重複していたとします。したがって、パブリック IP アドレスが同じなため、NAT IP アドレスが Unified Communications Manager アプリケーション間でクロス起動する場合があります。

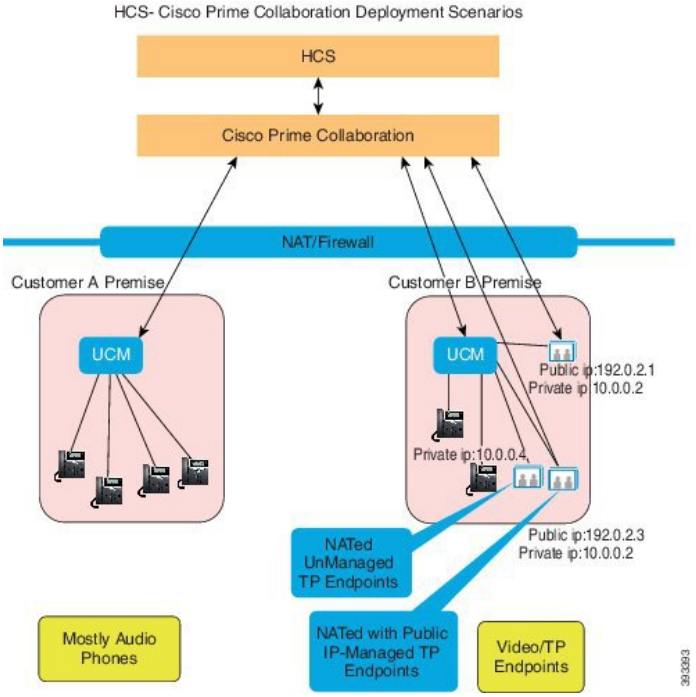
次の図には、NAT 環境での、HCS-Cisco Prime Collaboration Assurance の導入シナリオが示されています。

（注） 次の図は、Cisco Prime Collaboration Assurance Release 11.1 以前のバージョンに適用されます。

図 *1 : Cisco Prime Collaboration* の導入シナリオ



（注） 次の図は、Cisco Prime Collaboration Assurance Release 11.5 以降のバージョンに適用されます。



音声とビデオの Unified Dashboard

それぞれのカスタマーを分離して、音声とビデオのコラボレーション ネットワークのエンドツーエンド モニタリングができます。

各カスタマーのネットワークについて、次の内容の詳細および概要を表示できます。

- Cisco Unified Communications Manager および Cisco Video Communication Server クラスタの概要情報
- 会議とアラーム
- デバイスの詳細
- 各管理対象デバイスのパフォーマンス
- Contact Center のコンポーネント（Cisco Unified Intelligence Center（CUIC）、Cisco Finesse、Cisco MediaSense、Cisco Unified Customer Voice Portal（Cisco CVP）、Cisco Unified Contact Center Enterprise（Unified CCE）など）の情報

/[デバイスインベントリ（Device Inventory）]/[インベントリ管理（Inventory Management）]

HCS 特有の検出の詳細については、「HCS ドキュメント」を参照してください。

各お客様の インベントリを個別に表示および管理することができます。

デバイスを検出するカスタマーを選択できます。非 NAT 環境では、パブリック IP（管理 IP）には検出された IP アドレスが入力され、プライベート IP にはデフォルトでパブリック IP（管理 IP）が入力されます。

ユーザはデバイスとクラスタを検出し、それらを特定のカスタマーに関連付けることができます。管理されている既存のすべてのエンドポイント、またはパブリッシャに登録されているサブスクライバが、パブリッシャからカスタマー名を継承するかどうかを選択できます。

Cisco Unified Communications Manager（電話機や Cisco TelePresence）、Cisco Expressway（Cisco TelePresence）、Cisco TMS（Cisco TelePresence）に登録されている、すべてのエンドポイントを検出および管理することができます。エンドポイントの管理に加えて、カスタマーの音声およびビデオコラボレーションネットワークに含まれる、マルチポイント スイッチ、アプリケーション マネージャ、コール プロセッサ、ルータ、スイッチも管理できます。

検出では、デバイス インターフェイスと周辺機器の詳細も取得され、Cisco Prime Collaboration Assurance に保存されます。

音声およびビデオのエンドポイント モニタリング

ビデオのエンドポイントの場合、Cisco Prime Collaboration Assurance では、各顧客用にすべてのポイント ツー ポイント、マルチポイント、マルチポイントのビデオ コラボレーション会議を監視することができます。これらの会議は、次のいずれかのステータスとともにアドホック、スタティック、またはスケジュール済みとなります。

- In-progress
- Scheduled

- Completed
- No Show

診断

複数の診断テストを実行して、個々のカスタマーの UC 電話ネットワークに関連する問題を特定できます。

NAT 環境では、パブリック IP アドレスを備えたエンドポイントでのみ Medianet がサポートされます。NAT 環境では、ビデオ 会議の診断は、パブリック IP アドレスを持つエンドポイントのみサポートしています。

Cisco Prime Collaboration リリース 11.5 以降の場合

Cisco Medianet テクノロジはサポートされていません。

障害管理

複数のカスタマーのアラームとイベントを個別にモニタできます。また、イベントの重大度をカスタマイズできるほか、その重大度に基づいて Cisco Prime Collaboration Assurance から通知を受け取ることもできます。

カスタマー特有のデバイス通知グループも作成できます。

レポート

個々のカスタマーに対して事前に定義されているレポートとカスタマイズ可能なレポートは、すべて使用できます（ただし NAM や Sensor レポートなどのセンサーベースのレポートは除きます）。

Enterprise モードと MSP モードの詳細については、Enterprise モードと MSP モードの違い （24 ページ）を参照してください。

Cisco Prime Collaboration Analytics

Cisco Prime Collaboration リリース 11.5 以降の場合

Cisco Prime Collaboration Analytics でサポートされている新機能は、次のとおりです。

- **グローバル顧客選択**：Cisco Prime Collaboration Analytics のホームページで、必要に応じてお客様を選択して情報をフィルタリングすることができます。
- **スケジュール設定済みレポート**：スケジュール設定済みレポートでは、複数のお客様の選択がサポートされています。生成されたレポートには、複数のお客様のデータが含まれています。
- **ロゴ管理**：お客様は、ロゴをアップロード、交換、削除できます。アップロードしたロゴはスケジュール設定済みレポートに含まれます。
- **ロール ベース アクセス制御**：レポート ビューア ロールは、キャパシティ分析、ライセンス使用状況、マイ ダッシュボード以外のすべてのダッシュボードでサポートされていま

す。レポート ビューアではレポートをスケジュールすることはできず、[スケジュール済みレポート（Scheduled Reports）] メニューにアクセスすることもできません。

Enterprise モードと MSP モードの違い

Cisco Prime Collaboration Assurance に提供される機能は、次の表に記載されている相違点を除き、Enterprise および MSP モードでは同じです。

マネージド サービス プロバイダー（MSP）モード	Enterprise モード
Advanced モードでのみ提供されます。	Advanced の両モードがあります。
カスタマーを作成し、カスタマーに特定のデバイスを追加できます。	企業では、ドメインと呼ばれる論理ユニットを作成できます。これはAdvancedモードのオプション機能です。
情報を、顧客、インベントリ管理、電話機のインベントリ レポート、会議およびエンドポイントの診断別にフィルタリングします。	情報を、ドメイン別、ならびにインベントリ テーブルではインベントリ管理、会議およびエンドポイントの診断別にフィルタリングします。
および[顧客概要（Customer Summary）]でダッシュボードとダッシュレットを提供します。 **Cisco Prime Collaboration リリース 11.5 以降の場合** Cisco TelePresence Exchange（CTX）は利用が停止されました。	および[顧客概要（Customer Summary）]でダッシュボードとダッシュレットは提供されません。
特定のカスタマーのルータおよびスイッチに対して IP SLA テストを実行できます。	Ip SLA テストは、IP SLA 対応のルータとスイッチで利用できます。
CTXクラスタ、およびCTXでサポートされるミーティングタイプのサポートを提供します。 **Cisco Prime Collaboration リリース 11.5 以降の場合** Cisco TelePresence Exchange（CTX）は利用が停止されました。	CTX をサポートしません。
カスタマー グループに対してロールベース アクセス コントロール（RBAC）を提供します。	Assuranceデバイス プールおよびエンドポイントに対してロールベース アクセス コントロール（RBAC）を提供します。
スタティック NAT をサポートします。	NAT をサポートしません。

マネージド サービス プロバイダー（MSP）モード	Enterprise モード
ホスト型および非ホスト型の両方の導入モデルで CTX 管理機能をサポートします。 **Cisco Prime Collaboration リリース 11.5 以降の場合** Cisco TelePresence Exchange（CTX）は利用が停止されました。	CTX をサポートしません。
RTP ベースの診断テスト（Synthetic テストなど）は非 NAT 環境でのみサポートされます。	すべての機能がサポートされています。
NAT 環境の電話機では、Phone XML で検出されたデータは利用できません。ビデオ会議の統計と会議情報は、[Full Visibilty] に設定されていても、電話機では利用できません。	すべての機能がサポートされています。
センサーベースのコール品質レポートは使用できません。	すべてのレポートを使用できます。
NAT 環境では、Cisco TelePresence エンドポイントのヘルス モニタリングは、パブリック IP アドレスを備えた Cisco TelePresence エンドポイントでのみサポートされます。	すべての機能がサポートされています。
NAT 環境では、ビデオ会議および会議の診断は、パブリック IP アドレスを持つエンドポイントのみサポートしています。	ビデオ会議の診断の全機能がサポートされています。
自動検出はサポートされません。	自動検出はサポートされています。
Cisco Prime Collaboration リリース 11.5 以降の場合 FIPS 準拠はサポートされていません。 **Cisco Prime Collaboration リリース 12.1 以降の場合** FIPS 準拠はサポートされていません。	**Cisco Prime Collaboration リリース 11.5 以降の場合** FIPS 準拠はサポートされています。 **Cisco Prime Collaboration リリース 12.1 以降の場合** FIPS 準拠はサポートされていません。
Cisco Prime Collaboration リリース 11.5 以降の場合 Perimeta Session Border Controller（SBC）はサポートされています。	Perimeta Session Border Controller（SBC）はサポートされていません。

マネージド サービス プロバイダー（MSP）モード	Enterprise モード
NAT 環境では、パブリック IP アドレスを備えたエンドポイントでのみ Medianet がサポートされます。 **Cisco Prime Collaboration リリース 11.5 以降の場合** Cisco Medianet テクノロジはサポートされていません。	Medianet のすべての機能がサポートされます。 **Cisco Prime Collaboration リリース 11.5 以降の場合** Cisco Medianet テクノロジはサポートされていません。
Cisco Prime Collaboration リリース 11.5 以降の場合 SFTP サーバにアップロードされた Scheduled Reports の場合、レポートへのアクセスは Scheduled Reports を作成したユーザに制限されます。	**Cisco Prime Collaboration リリース 11.5 以降の場合** sFTP サーバにアップロードされた Scheduled Reports では、すべてのユーザがレポートを表示できます。
Cisco Prime Collaboration リリース 11.6 以降の場合 Credential Profile 機能はサポートされていません。	Credential Profile 機能はサポートされています。

Cisco Prime Collaboration Assurance NBI

Cisco Prime Collaboration Assurance NBI は、次の点ものをサポートしています。

- デバイスの管理
- デバイス クレデンシャルを表示および削除します。
- フィルタ条件に基づきすべてのビデオ セッションを一覧表示します。
- ビデオ セッションをトラブルシュートします。
- Unified CM クラスタからエンドポイント数を取得します。

  。
- フィルタ条件に基づきアラームを一覧表示します。

Cisco Prime Collaboration リリース 11.5 以降の場合

トラブルシューティングはサポートされていません。

NB API ドキュメントにアクセスするには、管理者権限で Cisco Prime Collaboration Assurance サーバにログインし、ブラウザ URL に次のとおりに入力します。

```
http://<pc-server-ip>/emsam/nbi/nbiDocumentation
```

*<pc-server-ip>*は Cisco Prime Collaboration Assurance サーバの IP アドレスです。

Cisco Prime Collaboration リリース 11.6 以降の場合

NB API ドキュメントにアクセスするには、Cisco Prime Collaboration Assurance サーバにログインし、ユーザ インターフェイスの右上隅にある [設定（Settings）] のドロップダウン メニューから **[Assurance NB API ドキュメント（Assurance NB API documentation）]** を選択します。

Cisco Prime Collaboration リリース 12.1 以降の場合

```
https://<pc-server-ip>:<port-number>/emsam/nbi/nbiDocumentation
```

<pc-server-ip> はサーバの IP アドレスであり、*<port-number>* は HTTP ポート番号です。

例：

```
https://<pc-server-ip>:8443/emsam/nbi/nbiDocumentation
```

これらの NBI とは別に、アラームまたはイベントが発生するたびに、SNMP トラップ（CISCO-EPM-NOTIFICATION-MIB）をトラップの受信者に送信するよう設定できます。

Cisco Prime Collaboration Assurance および Analytics の Geo-Redundancy

Cisco Prime Collaboration Assurance および Analytics は、VMware vSphere レプリケーションにより地域の冗長性をサポートします。Geo-Redundancy を設定するため、追加の Cisco Prime Collaboration Assurance and Analytics ライセンスは必要ありません。Geo-Redundancy の詳細については、「Cisco Prime Collaboration Assurance および Analytics 用の Geo Redundancy」を参照してください。

新機能および変更された機能に関する情報

次の表には、12.1 Service Pack 1 のリリース用として、このガイドで追加または変更された情報が示されています。

Table 2: **新機能および変更された機能に関する情報**

日付	更新内容
2018 年 4 月 10 日	TLS v1.2 通信プロトコルのサポート
2018 年 5 月 14 日	CUCM でセキュアな JTAPI 通信をサポートするための新しいフィールド
2018 年 7 月 4 日	セッション監視用のセキュアな JTAPI 通信

次の表には、12.1のリリース用として、このガイドで追加または変更された情報が示されています。

Table 3: 新機能および変更された機能に関する情報

日付	更新内容
2017 年 7 月 21 日	Cisco Prime Collaboration Assurance セクションに [新機能（What's New）] を追加しました。
2017年3月13日	[デバイス ステータスの概要（Device Status Summary）]に関する情報が更新されました。
2017 年 3 月 14 日	「クラスタのセットアップ」章にある TMS クラスタの既存のコンテンツが変更されました。
2017 年 3 月 27 日	Audio Phone Report と Video Phone Audit Report が 1 つの Endpoint Move Report へとマージされました。
2017 年 3 月 31 日	Audio Phone Report と Video Phone Move Report が 1 つの Endpoint Move Report へとマージされました。
2017 年 4 月 24 日	Removed IP Phone Report と Removed Video Phone Report が 1 つの Endpoint Move Report へとマージされました。
2017 年 5 月 30 日	Audio Extension Report と Video Extension Report が 1 つの Endpoint Move Report へとマージされました。
2017 年 4 月 5 日 2017 年 4 月 17 日	各ユーザ インターフェイスにいくつかの変更を加えました。 1. デバイスを削除するため依存関係を処理 2. CUBE SIP トランク：セッション サーバ グループ設定の変更
2017 年 3 月 23 日	Cisco Prime Collaboration Assurance からデバイスを削除したときに、削除されたデバイスについて、「デバイスの再検出」セクションの情報が更新されます。

日付	更新内容
2017 年 6 月 6 日	PIFServer を削除するプロセスの一部として、[インベントリ スケジュール（Inventory Schedule）] ページから [IP Phone Inventory Collection] および [IP Phone XML Collection] が削除されます。この変更では、次のことに対応しています。 **1.** 「システム パラメータの設定」、「クラスタ データ検出のスケジュール」、「インベントリ詳細の更新と収集」、「インベントリ詳細の収集」、「グローバル システム パラメータ」セクションの情報を更新しました。 **2.** 「IP Phone Discovery Schedule」と「Schedule IP Phone XML Discovery Schedule」セクションを削除しました。
2017 年 6 月 6 日	CME の syslogs 設定の説明を記載した、「Cisco Unified CME の Syslog メッセージを使用して IP フォンを監視する」セクションが追加されました。
2017 年 6 月 6 日	「インベントリの登録済みエンドポイントに関するライセンス」で行った変更を説明するため、「ライセンス数」セクションを更新しました。
2017 年 6 月 26 日	「ジョブのスケジュール」セクションを修正し、[ジョブ管理ページの設定ボタンを修正」に関する問題を説明するため、新たに「タイムテーブルの定義」セクションを追加しました。
2017 年 6 月 26 日	30 日以上前のデータが毎日削除されることを含む、すべての監査レポートに関する変更は、「バックアップと復元の実行」および「パージ ポリシー」の表に記載されています。
2017 年 6 月 26 日	「Cisco Prime Collaboration Assurance のライセンス ユーザ インターフェイスでは、各プロファイル（Small/Large/BE6k）に基づきインポートできるライセンスの最大数を制限する必要があります」の変更点を特定するため、「ライセンスの管理およびライセンス詳細の表示」セクションに情報を追加しました。
2017 年 6 月 1 日	Data Migration Assistant Tool によるスキーマ変更の取り扱いに問題を特定するため、「Cisco Prime Collaboration Assurance のアップグレード」セクションに注記を追加しました。
2017 年 6 月 1 日	FIPS コンプライアンスに関するすべてのオカレンスが非表示になりました。isco Prime Collaboration Assurance 12.1 Enterprise の一部として、FIPS コンプライアンスは保証されていません。「FIPS コンプライアンスの有効化」セクション全体が非表示になりました。

日付	更新内容
2017 年 3 月 21 日	SFTP クレデンシャルのユーザ インターフェイスに関するナビゲーションが変更されています。「システム パラメータの設定およびシステム パラメータ上の表」セクション、ならびに対応する「sFTP設定の構成」セクションが変更されています。

Cisco Prime Collaboration Assurance の新機能

Cisco Prime Collaboration Assurance 12.1 Service Pack 1 の機能は Cisco.com からアクセスできます。

***Table 4: Cisco Prime Collaboration Assurance 12.1 Service Pack 1* の機能**

機能名	機能説明
TLS v1.2	Cisco Prime Collaboration Assurance のサーバおよびクライアント インターフェイスの両方では、TLS v1.2 通信をサポートします。
CUCM でセキュアな JTAPI 通信をサポートするための新しいフィールド	[インベントリ管理（Inventory management）] ページで [デバイスの追加（Add Device）]、[クレデンシャルの変更（Modify Credentials）]、[クレデンシャルの管理（Manage Credentials）] の JTAPI セクションが変更されました。このセクションには、TLS v1.2 上で CUCM を使用した セキュアな JTAPI 通信をサポートする 7 つの新しいフィールドがあります。
セッション監視用のセキュアな JTAPI 通信	Cisco Prime Collaboration Assurance のセッション監視機能（会議の監視）に、TLS v1.2 上で CUCM を使用したセキュアな JTAPI 通信のプロトコル オプションが導入されました。
合成テスト用のセキュアな JTAPI 通信	Cisco Prime Collaboration Assurance の合成テスト機能に、TLS v1.2 上で CUCM を使用したセキュアな JTAPI 通信のプロトコル オプションが導入されました。

Note 会議の診断と音声電話機能の模擬テストを正しく実行するには、Cisco Prime Collaboration Assurance Service Pack 1 バンドルを適用する前に、CUCM がリストされているバージョンであることを確認してください。詳細については、12.1 SP1 の『Cisco Prime Collaboration Assurance でサポートされているデバイス』を参照してください。

Cisco Prime Collaboration Assurance 12.1 の機能には、Cisco.com からアクセスできます。

***Table 5: Cisco Prime Collaboration Assurance 12.1* の機能**

機能名	機能説明
インベントリ：デバイス ステータスの概要	アンマネージド カウントの修正：ヘッダーのアンマネージド カウントは、[デバイス ステータスの概要（Device Status Summary）] ページのカウントと一致する必要があります。両方のカテゴリのカウントが、この条件を満たす必要があります。
インベントリ：TMS クラスタ	TMS 検出では、Cisco Prime Collaboration Assurance が CUCM または VCS デバイスを管理しなくても、TMS をプロビジョニングしたすべてのデバイス（CUCM/VCS/endpoint/MCU/TPS/TP_Conductor）を検出します。ただし、TMS 検出では、CUCM/VCS/エンドポイントが論理的に検出されることはありません。

機能名	機能説明
レポート	次のレポートが 1 つのレポートにマージされました。 **1.** Endpoint Audit Report は、Audio Phone Report と Video Phone Audit Report が 1 つになったレポートです。**ナビゲーション**：[レポート（Reports）] -> [その他のレポート（Miscellaneous Reports）] -> [Endpoint Audit Report] **2.** Endpoint Move Report は、Audio Phone Report と Video Phone Move Report が 1 つになったレポートです。**ナビゲーション**：[レポート（Reports）] -> [その他のレポート（Miscellaneous Reports）] -> [Endpoint Move Report）] **3.** Endpoint Remove Report は、Removed IP Phone Report と Removed Video Phone Report が 1 つになったレポートです。**ナビゲーション**：[レポート（Reports）] -> [その他のレポート（Miscellaneous Reports）] -> [Endpoint Remove Report）] **4.** Endpoint Extension Report は、Audio Extension Report と Video Extension Report が 1 つになったレポートです。**ナビゲーション**：[レポート（Reports）] -> [その他のレポート（Miscellaneous Reports）] -> [Endpoint Extension Report）]

機能名	機能説明
ユーザ インターフェイスの変更	次は、各ユーザインターフェイスの変更点です。 **1.** デバイス削除時の依存関係：パブリッシャ、サブスクライバ、VCS、TMS、ESX、VCENTER、TPS、UNITY CONNECTION、MULTIPOINT コントローラ、IM&P などを含むデバイス、ならびんにその他のインフラストラクチャ デバイスとそれらに関連付けられたエンドポイントは、[State] 状態が削除されるとデータベースから削除されます。 **2.** CUBE SIP トランク：セッション サーバ グループ設定の変更 「セッション サーバ グループ設定」の付いた CUBE SIP トランクを表示するには、[Collaboration ネットワーク管理による使用率の監視へのアクセス（Collaboration Network Administrator access the Utilization Monitor）] -> [CUBE SIP トランク（CUBE SIP Trunk）] タブの順に移動します。サーバ グループの場合、この画面には、Dialpeer から SIP トランクまでの 1 つおよび複数の設定をサポートする際の、制限に関する情報が提供されます。サーバ グループ設定では、イベントを発生/抑制するオプションもあります。
	Cisco Prime Collaboration Assurance の削除時にデバイスを削除 このアップデートには、管理者がデバイスを再検出する前に、デバイスを追加する必要があることについての説明があります。デバイスを削除する際に、Cisco Prime Collaboration Assurance からデバイスを削除します。

機能名	機能説明
	[インベントリ スケジュール（Inventory Schedule）] ページから IP Phone Inventory Schedule および IP Phone XML Inventory Schedule を削除します。 Cisco Prime Collaboration Assurance Enterprise/MSP モードから PIFServer を削除すると、IP Phone Inventory Collection および IP Phone XML Collection 検出も削除されます。この変更では、次のことに対応しています。 **1.** [インベントリ スケジュール（Inventory Schedule）] -> [IP Phone Inventory Schedule および Inventory Schedule（IP Phone Inventory Schedule and Inventory Schedule）] -> [IP Phone XML Discovery 検出（IP Phone XML Discovery）] ページが削除されました。 **2.** [インベントリ（Inventory）] タブの [Inventory Schedule] が [Cluster Data Discovery Schedule] へと名前変更されました。
CME Syslog	ここでは、CME で syslogs を設定する手順を説明します。この syslogs は、Cisco Unified CME Syslog メッセージを使用した IP フォンの監視に役立ちます。
インベントリの登録済みエンドポイントのライセンス	最初に、特定のクラスタ内にある最新の登録済みエンドポイントをパージします。登録済みのエンドポイントをクラスタ名別に並べ替え、クラスタを識別し、ライセンス要件を満たすためパージします。電話機のライセンスをインベントリ モジュールに移植する間に、Cisco Prime Collaboration Assurance から PIFServer を削除します。
[Job Management（ジョブ管理）] ページの [設定（Settings）] ボタンに関するの問題の修正	[ジョブの詳細（Job Details）] ペインの [スケジュール（Schedule）] や [設定（Settings）] タブを使用して、ジョブをスケジュールおよびオプションを設定します。
監査レポートは 30 日後にパージ	コール品質イベントの履歴とエンドポイント関連（音声/ビデオ電話はエンドポイント関連のもので置き換え）の監査レポートデータは、30 日を経過するとパージされます。

機能名	機能説明
Cisco Prime Collaboration Assurance ライセンス ユーザ インターフェイスでは、Small、Large、BE6k などの各プロファイルに基づき、インポートできるライセンスの最大数を制限する必要があります。	Cisco Prime Collaboration Assurance ライセンスでは、サポートしている数よりも多くのライセンスファイルをアップロードすることができます。たとえば、Small から 3K のエンドポイントです。Cisco Prime Collaboration Assurance が、1 つのプロファイルでサポートしている最大カウント数よりも少ないエンドポイントを持つライセンス ファイルを受け入れた場合は、ユーザにエラー メッセージを通知する必要があります。 これは、Assurance Mass、Contact Center Assurance、Analytics ライセンスに適用され、Small/Medium/Large/Very Large/BE6k/BE7K などのすべてのプロファイルをサポートしています。
DMA を介したスキーマ変更の処理	11.x（11.0、11.1、11.5、11.6）から 12.1 にアップグレードするときには、インベントリの周りのスキーマが変更されます。アップグレード中には、11.x で利用可能ないくつかのデータベース関連のテーブル列が削除されます。Cisco Prime Collaboration Assurance の全体機能には影響しません。 [Deleted] 状態のデバイス/エンドポイントはパージされ、アップグレード後には利用できません。
FIPS ユーザ インターフェイスの非表示	isco Prime Collaboration Assurance 12.1 Enterprise の一部として、FIPS コンプライアンスは保証されていません。このため、[System Administration（システム管理）] ページで FIPS を有効/無効にするセットアップ メニューは非表示になっています。

機能名	機能説明
sFTP クレデンシャル ユーザ インターフェイスの実装	ユーザ インターフェイスに [CUCM sFTP クレデンシャル（CUCM sFTP Credentials）] や [保存（Save）] などのボタンが追加されました。同じユーザのパスワードを変更するためのチェックボックスと、パスワード オプションを確認するためのオプションを使用できます。 ナビゲーションが [アラームとレポート管理（Alarm & Report Administration）] -> [CDR ソース設定（CDR Source Settings）] -> [CUCM SFTP クレデンシャル（CUCM SFTP Credentials）] から[インベントリ（Inventory）] -> [インベントリ管理（Inventory Management）] -> [CUCM sFTP クレデンシャル（CUCM sFTP Credentials）] に変更
RTMT Polling Inconsistency の実装：警告およびイベント用のメモ	マルチ ノードのコール マネージャ クラスタでは、同じアラートが複数のノードで同時に存在する場合、Cisco Prime Collaboration Assurance は最新アラートを 1 つのみ表示します。
電話機からエンドポイントで未登録のしきい値	「未登録の電話機」から「未登録のエンドポイント」へと変更されました。
プロセスの説明列：有用性	出力時にプロセスのステータスがわかるよう、各プロセスを示すプロセスの説明列が追加されました。
Prime Collaboration Assurance の Prime License Manager でライセンスの使用状況が表示されない	共存する PLM を管理しつつ、[監視（Monitor）] -> [使用率の監視（Utilization Monitor）] -> [ライセンスの使用状況（License Usage）] に移動して CLI と HTTP のクレデンシャルを提供します。管理者は、CLI クレデンシャルを使用してライセンス情報や HTTP クレデンシャルにアクセスし、Cisco Prime Collaboration Assurance の Prime License Manager を管理することができます。
[Inaccessible] ステータスが SNMP タイムアウトとして表示	VMware vCenter Server または UCS Manager が [インベントリ（Inventory）] -> [インベントリ管理（Inventory Management）] -> [クレデンシャルの管理（Manage Credentials）] タブを通して追加されると、HTTP クレデンシャルのみが必要であることを示す注記が追加されます。これらのデバイスで SNMP が必要ない場合、[Inaccessible State] 列には「SNMP timeout」と表示されます。

機能名	機能説明
スタンドアロン PLM が PCA 11.6 で non-Cisco として検出	この問題に対処するために、トラブルシューティング セクションが追加されました。 これは、PLM に SNMP コミュニティ文字列が設定されている場合に発生する可能性があります。PLM を適切に検出するには、コミュニティ文字列を設定しないようにします。コミュニティ文字列に設定されている場合は、文字列を削除し、Cisco Prime Collaboration Assurance で PLM を検出します。Cisco Prime Collaboration Assurance は、PLM の検出で SNMP コミュニティ文字列の設定はサポートしていません。
SFTP でレポートの生成後に PCA BACKUP ジョブのステータスでエラーが表示	この問題に対処するために、トラブルシューティング セクションが追加されました。 トラブルシューティング セクションには、ユーザ フォルダで GPG キーを生成する方法が示されています。
グローバル管理ユーザが破損しているため [OpsView ダッシュレット（OpsView Dashlet）] ページが読み込まれません	[トラブルシューティング セクションでは推奨処置とパスについて説明しています この問題を解決するには、新しいスクリプト（opsview_globaladmin.sh）と推奨されるパス（/opt/emms/emsam/bin）を利用します。
LDAP パラメータ値でアンパサンドが使用できない	この問題を解決するため、注記が追加されています。 LDAP に接続するため新しい LDAP パラメータ値（?CN=hq-prime,OU=Service Access Groups,DC=Megafon,DC=ru?）が定義されました。
スケジュールするには CME Discovery および Phone XML Discovery ジョブを制限	この問題を解決するため、注記が追加されています。 通常、CMEPhoneDiscovery および PhoneXML Discovery ジョブは 4 時間おきに実行するようスケジュールされています。これらのジョブは、再実行ではなく 1 回のみ実行するよう変更できます。検出後は、これをスケジュール設定に戻すことはできません。

機能名	機能説明
すべてのオクテットが正しく表示されない	Cisco Prime Collaboration Assurance 12.1 OVA の導入時には、IP アドレス、IP デフォルト ゲートウェイ、IP デフォルト ネットマスク、バックアップ サーバ IP に対して 3 つのオクテットのみが表示されます。4番目のオクテットは表示されません。すべてのオクテットを表示するには、[タブ（Tab）] ボタンを押します。
ドキュメントから [デバイス ステータスの概要（Device Status Summary）] の自動更新を削除	[デバイス ステータスの概要（Device Status Summary）]ページの動作が変更されています。ページは 30 秒ごとに自動更新されません。
このスクリプトをサーバ上で実行して CDR_CMR レポートの生成およびエクスポート	管理者のみが CDR/CMR レポートをエクスポートできます。スクリプトを作成して、サーバ上でエクスポートのタスクを自動化します。
NBI API に関するマニュアル	Sample Input コードの確認と修正。
Device 360 のパフォーマンス データ	[デバイス 360（Device 360）] ビューでパフォーマンス データは表示されません。その代わり、[ここをクリックしてパフォーマンスデータを表示（Click here for performance data）] リンクをクリックすると、同じデータが表示されます。
Ops ビュー クラスタ概要のパフォーマンス データ	[Call Health Summary] タブに列が追加されました。
このリリースからサポートの対象外となる機能またはデバイス	**1.** Cisco TelePresence-Manager（CTS-Manager/CTS-MAN）デバイスはサポートされていません。そのため、ドキュメントからデバイスのすべてのオカレンスが削除されました。 **2.** FIPS 準拠はサポートされていません。そのため、ドキュメントからすべてのオカレンスが削除されました。 **3.** ドキュメントから CTX 固有のコンテンツが削除されました。 **4.** [論理検出の有効化（Enable Logical Discovery）] ボタン：ドキュメントから論理検出を有効にするボタンが削除されました。 **5.** CLI はサポートされません。そのため、ドキュメントから CLI 固有のコンテンツが削除されました。

機能名	機能説明
一般	1. 「Cisco Prime Collaboration」から「Cisco Prime Collaboration Assurance」に名前変更されました。 2. 「PhoneUnregThresholdExceeded」から「EndpointUnregThresholdExceeded」に名前変更されました。
Mixed モードでの UCM のサポート	Cisco Prime Collaboration Assurance は、混合モードの Cisco Unified CM クラスタをサポートしています。 ただし、次の Cisco Prime Collaboration Assurance の機能は、CUCM へのセキュリティで保護されていない通信に対してのみサポートします。 • セッション監視は、セキュリティで保護されていない JTAPI 通信を使用して、セッションを監視し続けます。 • 模擬テスト：セキュアモードで CUCM に登録されている CUCM およびエンドポイントへの、セキュアなシグナリング（TLS）およびセキュアなメディア（SRTP）接続はサポートしません。

Cisco Prime Collaboration Analytics の概要

このドキュメントでは、Cisco Prime Collaboration 11.0、11.1、11.5、11.6、12.1、12.1 SP1、12.1 SP2、12.1 SP3 の機能について説明します。

Cisco Prime Collaboration Analytics は、トラフィックの傾向、テクノロジの導入傾向、使用率が高いおよび低いリソース、ネットワークでのデバイスリソースの使用状況を識別することができます。また、断続的および繰り返し発生するネットワークの問題を追跡し、Cisco Prime Collaboration Analytics ダッシュボードを使用してサービスの品質問題も特定できます。

デフォルトでは、Cisco Prime Collaboration Analyticsは Cisco Prime Collaboration Assurance アプリケーションとともにインストールされます。Analytics は無効にすることも、Analytics の評価ライセンスの期限が切れるまで使用することもできます。ただし、唯一の例外としては、非常に大きな OVA（150 K）をインストールする場合、Cisco Prime Collaboration Assurance のみをインストール、または Cisco Prime Collaboration Assurance を Cisco Prime Collaboration Analytics とともにインストールすることもできます。

インストールとシステム要件の詳細については、『Cisco Prime Collaboration Assurance および Analytics のインストールとアップグレードに関するガイド』を参照してください。

Cisco Prime Collaboration Analytics NBI

次は、Cisco Prime Collaboration Analytics 11.5 SP1、11.6、12.1、12.1 SP1 がサポートする NBI 機能です。

- 次のダッシュボードでは、NBI API サポートを利用できます。
  - キャパシティ分析
  - UC システム パフォーマンス
  - ビデオ会議の分析
  - ライセンスの使用状況
  - **Cisco Prime Collaboration リリース 11.6 以降の場合**

    Video Communication Server / Expressway

（注） Cisco Prime Collaboration Analytics Release 11.5 の一部として、次のダッシュボードでは NBI API がすでにサポートされています。

- テクノロジー導入
- 資産使用状況
- トラフィック分析
- サービス エクスペリエンス

Cisco Prime Collaboration リリース 11.6 以降の場合

NBI API は、[License Usage] ダッシュボードの [Video Communication Server / Expressway] ダッシュレットで使用できるようになりました。

- サポートされている命名規則は次のとおりです。
  - ダッシュレットの場合：

    `https://<PC Server>/emsam/nbi/<dashboard>/<dashletname>/summary/parameters`
  - 詳細ビューの場合：

    `https://<PC Server>/emsam/nbi/<dashboard>/<dashletname>/details/dvparameters`
- NBI API ドキュメントには、パラメータの説明や NBI のサンプル URL が含まれています。NBI API ドキュメントにアクセスするには、管理者権限で Cisco Prime Collaboration Analytics サーバにログインし、次のいずれかの URL をブラウザに入力します。
  - `https://<pc-server-ip>/emsam/nbi/nbiAnalyticsDoc/`

    <*pc-server-ip*> はサーバの IP アドレスです。

- または

  ```
  https://<pc-server-ip>:<port-number>/emsam/nbi/nbiAnalyticsDoc/
  ```

  <pc-server-ip> はサーバの IP アドレスであり、*<port-number>* は HTTP ポート番号です。

  例：

  ```
  https://<pc-server-ip>:8443/emsam/nbi/nbiAnalyticsDoc/
  ```

- NBI URL で使用可能なパラメータは、GUI フィルタのパラメータとほぼ同じです。パラメータ名と値については NBI API ドキュメントを確認してください。

  （注） Cisco Prime Collaboration Analytics 11.5 の NBI API では、大文字と小文字が区別されないパラメータ値はサポートされていません。

- Call Detail Records（CDR）の NBI サポート：
  - NBI は、CDR ベース ダッシュレット用のレコードのクエリもサポートしています。

    ```
    https://<PC Server>/emsam/nbi/fetchCDR/fetchTableDetails
    ```

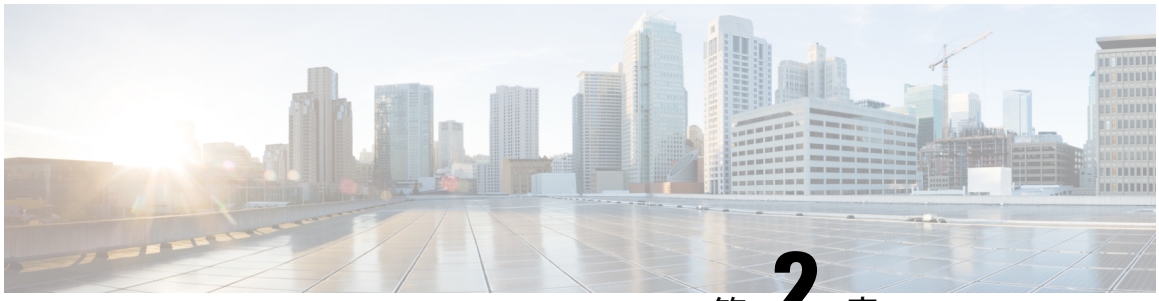
  - 結果には、CDR ベース ダッシュレットで凡例を選択したときにポップアップする、**詳細ビュー** のテーブルと類似した情報があります。
  - 検索条件は、次のフィルタの 1つを使用、または組み合わせることができます。
    - **コール**：ステータス、グレード、クラスタ、クラス、タイプ
    - **発信元エンドポイント**：dn、ip、uri、クラスタ/ロケーション、クラスタ/デバイス プール、ユーザ名、コーデック、エンドポイント モデル、エンドポイント タイプ
    - **送信先エンドポイント**：dn、ip、uri、クラスタ/ロケーション、クラスタ/デバイス プール、ユーザ名、コーデック、エンドポイント モデル、エンドポイント タイプ

- NBI API では、大文字と小文字を区別しないパラメータ値がサポートされています。たとえば、パラメータ「*timePeriod*」では、値として *last7days*、*Last14Days*、*last7DAYS* などを使用することができます。
- Cisco Prime collaboration Analytics Release 11.5 の一部として、NBI API は、CDR ベース ダッシュレット用の Call Detail Records（CDR）のクエリをサポートしています。詳細については、「Call Detail Records (CDR) NBI のサポート」を参照してください。

Cisco Prime Collaboration リリース 11.6 以降の場合

NB API ドキュメントにアクセスするには、Cisco Prime Collaboration Assurance サーバにログインし、ユーザ インターフェイスの右上隅にある [設定（Settings）] のドロップダウン メニュー

から**[Assurance NB API ドキュメント（Assurance NB API documentation）]** をクリックします。



第 2 章

概要

ここでは、次の内容について説明します。

- 概要 （43 ページ）

概要

この章では、Cisco Prime Collaboration Assurance の重要な概念について説明します。

イベント

イベントは、特定の時点で発生する別個の問題です。

各イベントは次のいずれかに該当します。

- ネットワークにおけるエラー、故障、異常事態など何らかの障害に伴うもの。たとえば、デバイスが到達不能になると、到達不能イベントがトリガーされます。
- 障害の解消に伴うもの。たとえば、デバイスの状態が到達不能から到達可能に変更されると、イベントがトリガーされます。

イベントの例には次のものがあります。

- ポート ステータスの変化
- ノードのリセット。
- ノードが管理ステーションに対して到達可能になる。
- ピア ルータでのルーティング プロトコル プロセス間の接続損失。

イベントは着信トラップおよび通知から取得され、ステータス変更（ポーリングによって）およびユーザ処理が検出されます。

イベントをトリガーした条件が存在しなくなっても、発生したイベントのステータスは変更されないことを理解することが重要です。

選択 **[モニタ（Monitor）]** > **[アラーム & イベント（Alarms & Events）]** をクリックして、イベントのリストを表示します。

アラーム

アラームは、障害のライフ サイクルを表したものです。

アラームの特性は、次のとおりです。

- 受信したイベントに対する Cisco Prime Collaboration Assurance の応答です。
- それぞれがアラームのライフ サイクルの特定の発生を表す一連のイベントです（次の例を参照）。イベントの順序では、重大度が最も高いイベントが、アラームの重大度を決定します。
- ネットワークで発生するエラー障害を示す一連の相互に関係するイベントを表します。
- アラームが発生したとき（障害が最初に検出されたとき）から、クリアされ、確認されるまでの完全なイベントのライフ サイクルを示します。

イベントの順序では、重大度が最も高いイベントが、アラームの重大度を決定します。

Cisco Prime Collaboration Assurance では、一連の相互に関係するイベントからアラームが作成されます。アラームの完全なイベントの順序には、少なくとも次の2つのイベントが含まれます。

- アラームのアクティブ化（インターフェイス ダウン イベントによってアラームが発生するなど）。
- アラームのクリア（インターフェイス アップ イベントによってアラームがクリアされるなど）。

アラームのライフサイクルには、重大度の変更、サービスへの更新などによってトリガーされる相互に関係するイベントをいくつでも含めることができます。

新しい関連イベントが発生すると、Cisco Prime Collaboration Assurance はそのイベントをアラームに関連付け、この新しいイベントに基づいてアラームの重大度およびメッセージテキストを更新します。手動でアラームをクリアすると、アラーム重大度の変更がクリアされます。

アラームを構成するイベントは、[Alarms and Events] ブラウザで確認できます。

選択 **[モニタ（Monitor）]** > **[アラーム & イベント（Alarms & Events）]** をクリックして、アラームのリストを表示します。

イベントの作成

Cisco Prime Collaboration Assurance は、イベント カタログを保持し、イベントをいつどのように作成するか、およびイベントをアラームに関連付けるかどうかを決定します。複数のイベントを同じアラームに関連付けることができます。

Cisco Prime Collaboration Assurance は、次の方法でイベントを検出します。

- 通知イベント（たとえば、Syslog やトラップ）を受信して、分析します。
- デバイスを自動的にポーリングして変更を検出します（たとえば、到達不能なデバイス）。
- アラームのステータスが変更されると（たとえば、ユーザがアラームをクリアすると）、イベントを受信します。

Cisco Prime Collaboration Assurance により、自分にとって重要ではないと考えられるイベントのモニタリングを無効にできます。無効になったイベントは、アラームおよびイベントのブラウザにリストされません。また、Cisco Prime Collaboration Assurance によってアラームがトリガーされることもありません。

syslog またはトラップとして受信した着信イベント通知は、事前に定義されたパターンとイベントデータとを照合することにより識別されます。イベントは、一致したパターンがあり、適切に識別できる場合に、Cisco Prime Collaboration Assurance によってサポートされていると見なされます。イベント データが事前定義済みのパターンと一致しない場合は、イベントはサポートされないと見なされ、ドロップされます。

次の表は、イベント作成を処理する間の Cisco Prime Collaboration Assurance の動作を示しています。

時刻	イベント	Cisco Prime Collaboration Assurance の動作
10:00AM PDT 2012年6月7日	デバイス A が到達不能になった。	デバイス A で新しい到達不能イベントを作成します。
10:30AM PDT 2012年6月7日	デバイス A は引き続き到達不能状態。	イベント ステータスに変更はありません。
10:45AM PDT 2012年6月7日	デバイス A が到達可能になった。	デバイス A で新しい到達可能イベントを作成します。
11:00AM PDT 2012年6月7日	デバイス A は到達可能なまま。	イベント ステータスに変更はありません。
12:00AM PDT 2012年6月7日	デバイス A が到達不能になった。	デバイス A で新しい到達不能イベントを作成します。

アラーム作成

アラームは、ネットワークにおける障害のライフサイクルを表します。複数のイベントを単一のアラームに関連付けることができます。

アラームは、次の順序で作成されます。

1. ネットワークで障害が発生すると、通知がトリガーされます。
2. この通知に基づいてイベントが作成されます。

3. このイベントに対応するアクティブなアラームがないかどうかを確認した後で、アラームが作成されます。

アラームは、次の 2 つのタイプのイベントに関連付けられます。

- アクティブイベント：クリアされていないイベント。アラームは、ネットワークで障害が解決されるまでこの状態のままです。
- 履歴イベント：クリアされたイベント。イベントは、障害がクリアされると、その状態を履歴イベントに変更します。アラームのクリア方法については、「アラーム ステータス」を参照してください。

アラームのライフサイクルは、アラームがクリアされると終了します。クリアされたアラームは、プリセット期間内に同じ障害が再発生した場合に復活されることがあります。

Cisco Prime Collaboration Assurance の場合、プリセット期間は 60 分です。

イベントとアラームの関連付け

Cisco Prime Collaboration Assurance によって、イベントとアラームのカタログが維持されます。カタログには、Cisco Prime Collaboration Assurance よって管理されるイベントのリストと、イベントとアラームの間の関係が含まれています。さまざまなタイプのイベントを同じアラームタイプに関連付けることができます。

通知の受信時には、次のことが行われます。

1. Cisco Prime Collaboration Assurance は、イベントとアラーム カタログに対する着信通知を比較します。
2. Cisco Prime Collaboration Assurance によって、イベントを発生させる必要があるかどうかが決定されます。
3. イベントが発生した場合、Cisco Prime Collaboration Assurance は、イベントが新しいアラームをトリガーするか、または既存のアラームに関連付けるかを決定します。

トリガーされる新しいイベントのタイプが同じで、同じソースで発生する場合、新しいイベントは既存のアラームに関連付けられます。

たとえば、アクティブなインターフェイス エラー アラームです。同じインターフェイスで発生するインターフェイス エラー イベントは、すべて同じアラームに関連付けられます。

イベントがクリアされると、重大度は情報に変更されます。

（注） 一部のイベントは、デフォルトの重大度が [Informational] になっています。このようなイベントには、アラームは作成されません。Cisco Prime Collaboration Assurance によってこれらのイベントのアラームを作成する場合は、イベントの重要度を変更する必要があります。

イベントの集約

一連の要素から受信した同じイベントの数が指定したしきい値を超えると、Cisco Prime Collaboration Assurance はアラームを作成します。

次に使用例を示します。

- デバイス プール/Unified CM の場所で登録解除された電話機の数が 5% を超えている。
- デバイス プール/Unified CM の場所でサービス品質の問題の数が 5% を超えている。
- 単一の低品質コールに対して生成されたすべてのコール品質イベントがグループ化されます。

イベント マスキング

Cisco Prime Collaboration Assurance では、最上位のコンポーネントが問題の原因である場合にイベントの階層が自動的にマスクされ、すべてのダウンストリームイベントがマスクされて、最上位コンポーネントに対するアラームが生成されます。

次に使用例を示します。

- Unified CM がダウンすると、Cisco Prime Collaboration Assurance によってそのすべてのコンポーネント（電源、インターフェイス、ファンなど）のイベントがマスクされる。
- スイッチ カードがダウンすると、Cisco Prime Collaboration Assurance によって含まれているすべてのポート レベルのイベントがマスクされる。

アラーム ステータス

次に、アラームでサポートされるステータスを示します。

表 *6 :* アラーム ステータス

ステータス	説明
Not Acknowledged	イベントが新しいアラームをトリガーしたか、イベントが既存のアラームに関連付けられる場合。
Acknowledged	アラームを確認すると、そのステータスは[Not Acknowledged] から [Acknowledged] に変更されます。

ステータス	説明
Cleared	• [System-clear from the device]：障害がデバイスで解決され、同じデバイスでイベントがトリガーされます。たとえば、デバイス到達可能イベントは、デバイス到達不能アラームをクリアします。 • アラームは、会議中にもパケット損失、ジッター、遅延によってトリガーされます。これらのアラームは、会議の終了後に自動的にクリアされます。 • [Cisco Prime Collaboration Assuranceユーザによる手動クリア（Manual-clear from Cisco Prime Collaboration Assurance users）]：ネットワークの障害を解決せずに、手動でアクティブ アラームをクリアできます。クリア イベントがトリガーされ、このイベントによってアラームがクリアされます。 • 引き続きネットワークに障害がある場合は、ポーリングに基づいて新しいイベントとアラームがさらに作成されます。 • [Cisco Prime Collaboration Assuranceサーバによる自動クリア（Auto-clear from the Cisco Prime Collaboration Assurance server）]：Cisco Prime Collaboration Assuranceは、会議の終了時に、会議に関するすべてのアラームをクリアします。 アクティブなアラームに対する更新が24時間ない場合、そのアラームはCisco Prime Collaboration Assuranceによって自動的にクリアされます。 （注） 特定のアラームは24時間前に自動的にクリアされる可能性があります。「Supported Events and Alarms for Prime Collaboration」を参照してください。

イベントの重大度

各イベントには重大度が割り当てられており、Cisco Prime Collaboration Assurance ではその色で識別できます。

イベントは、次の重大度カテゴリに大きく分類されます。

- フラグ付き：障害を示します。重大（赤）、やや重大（オレンジ）、比較的重大ではない（黄色）、または警告（空色）。
- 情報：情報（青）。一部の情報イベントは、フラグ付きイベントをクリアします。

イベントの順序では、重大度が最も高いイベントが、アラームの重大度を決定します。

Cisco Prime Collaboration Assurance では、イベントの設定および重大度をカスタマイズできます。各ユーザにとって重要なイベントには、それぞれより高い重大度を割り当てることができます。

イベントの設定および重大度がカスタマイズされていない場合は、Cisco Prime Collaboration Assurance アプリケーションで事前定義されているイベントの設定および重大度が使用されます。

イベントおよびアラームのデータベース

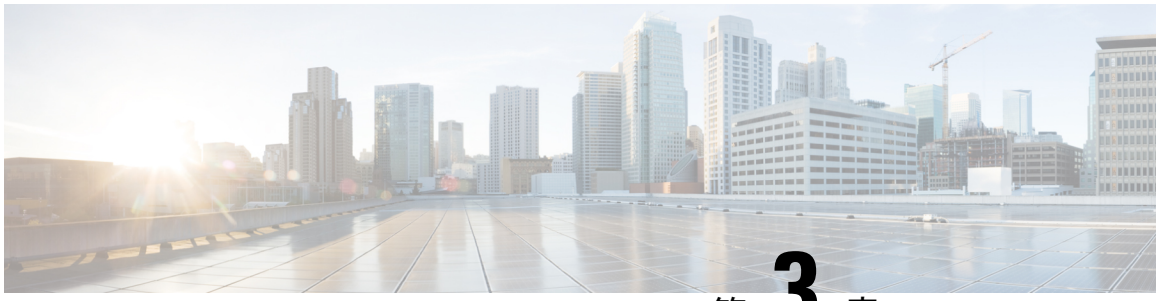
アクティブおよびクリアされたアラームを含むすべてのイベントとアラームは、Cisco Prime Collaboration Assurance データベースに保持されます。

イベント間の関係は保存されます。アラームおよびイベントブラウザでは、データベースの内容を確認できます。このデータの消去間隔は 4 週間です。

（注） イベントは、Cisco Prime Collaboration Assurance イベント オブジェクトの形式で保存されます。着信イベント通知（トラップまたは Syslog）の元の通知構造は維持されません。

アラーム通知

Cisco Prime Collaboration Assurance では、アラームの通知を受け取るように登録できます。Cisco Prime Collaboration Assurance は、ユーザが設定したアラーム セットと通知条件に基づいて通知を送信します。



第 3 章

Cisco Prime Collaboration Assurance を開始する

ここで紹介する例は、次のとおりです。

- Cisco Prime Collaboration Assurance を開始する （51 ページ）
- Cisco Prime Collaboration Analytics の開始 （56 ページ）

Cisco Prime Collaboration Assurance を開始する

Cisco Prime Collaboration Assurance は次のモードで利用できます。

- Cisco Prime Collaboration Assurance Enterprise モード
- Cisco Prime Collaboration Assurance MSP モード

。

（注） 次のセクションで説明するタスクを開始する前に、『Cisco Prime Collaboration Assurance and Analytics インストールおよびアップグレード ガイド』の「*Prime Collaboration Assurance* のインストール」セクションで説明されているタスクを完了する必要があります。

Cisco Prime Collaboration Assurance を開始する

Cisco Prime Collaboration Assurance をインストールした後、次の表に示すタスクを実行する必要があります。

表 *7 : Cisco Prime Collaboration Assurance* を開始する

アップグレード前	アップグレード後
	ホーム > 開始

<table>
<tr><th>アップグレード前</th><th>アップグレード後</th></tr>
<tr><td>ホーム > ネットワーク正常性の概要
• OPSView
• コール品質
• アラーム
• パフォーマンス
• Contact Center トポロジ</td><td rowspan="2">ネットワーク正常性の概要
• OpsView
• コール品質
• アラーム
• パフォーマンス
• Contact Center トポロジ

MSP モードでは、[顧客の概要（Customer Summary）のみを利用できます。</td></tr>
<tr><td>ネットワーク正常性の概要</td></tr>
<tr><td></td><td>モニタ
• アラームおよびイベント
• アラームの概要
• アラーム
• イベント
• 使用率モニタ
• T1/E1 トランク
• CUBE SIP トランク
• UCM SIP トランク
• ルート グループ
• トランク グループ
• Location CAC 帯域幅
• 会議デバイス
• Conductor Bridge Pool
• TelePresence エンドポイント
• ライセンスの使用状況（License Usage）</td></tr>
<tr><td>コール品質</td><td>NA</td></tr>
</table>

アップグレード前	アップグレード後
インベントリ（**Inventory**）	**Inventory** • インベントリ管理 • デバイス ステータスの概要 • **UC** デバイスの検索 • クラスタ デバイス • 検出スケジュール **Cisco Prime Collaboration Assurance 12.1 Service Pack 3** の場合 Cluster デバイスの検出スケジュール • **SNMP MIB** クエリ ツール
[インベントリ（**Inventory**）**] > [UC** デバイスの検索（**UC Device Search**）**]**	
[診断（**Diagnose**）**] > [**会議の診断（**Conference Diagnostics**）**]**	診断 • エンドポイントの診断 • 会議の診断 • **SIP Call Flow Analyzer** • **CME** 診断 • **Device Log Collector**
診断 **> SIP Call Flow Analyzer**	
[診断（**Diagnose**）**] > [**デバイス ログ コレクター（**Device Log Collector**）**]**	
模擬テスト • **UC Application Synthetic Test** • **Audio Phone Features Test** • **IP SLA Voice Test** • **Video Test** • **Phone Status Test** • **Batch Test**	模擬テスト • **UC Application Synthetic Test** • **Audio Phone Features Test** • **IP SLA Voice Test** • **Video Test** • **Phone Status Test** • **Batch Test**

アップグレード前	アップグレード後
レポート • 管理レポート • **CUCM** レポートの起動 • その他のレポート • 会議レポート • **TelePresence** エンドポイント レポート • **NAM & Sensor** レポート • **CDR & CMR** レポート • スケジュール済みレポート	レポート • **CDR** および **CMR** レポート • **NAM & Sensor** レポート • 会議レポート • **TelePresence** エンドポイント レポート • スケジュール済みレポート • 管理レポート • **CUCM** レポートの起動 • その他のレポート
	分析 • テクノロジー導入 • 資産使用状況 • トラフィック分析 • キャパシティ分析 • サービス エクスペリエンス • **UC** システム パフォーマンス • ビデオ会議の分析 • ライセンスの使用状況 • マイ ダッシュボード • カスタム レポート ジェネレータ • スケジュール済みレポート
Assurance レポート > 会議レポート • 会議の概要レポート • 会議の詳細レポート	

アップグレード前	アップグレード後
アラーム & レポート管理 • イベントのカスタマイズ • アラーム & イベント用の電子メール設定 • 通知のセットアップ • **CDR** ソース設定 • **CDR** 分析設定 • **1040** センサーのセットアップ • ポーリング設定 • **Customer Management**	アラーム & レポート管理 • イベントのカスタマイズ • アラーム & イベント用の電子メール設定 • 通知のセットアップ • **CDR** 分析設定 • **1040** センサーのセットアップ • 会議パスのしきい値設定 • ポーリング設定 • **APIC-EM & Prime Integration** **Cisco Prime Collaboration Assurance 12.1 Service Pack 3** の場合 **APIC-EM & NAM** • **Cisco Prime Collaboration Assurance 12.1 Service Pack 2** 以前の場合 **CDR** ソース設定 MSP モードでは、**[**顧客管理（**Customer Management**）**]** のみを利用できます。
システム管理 > ドメインのセットアップ	
	分析管理 • **sFTP** 設定 • グループ管理 • トランク トラフィックの最大キャパシティ設定 MSP モードでは、**[**顧客ロゴのアップロード（**Upload Customer Logo**）**]** のみを利用できます。

アップグレード前	アップグレード後
システム管理 • ライセンス管理 • ユーザ管理 • **[LDAP Settings]** • シングル サインオン • バックアップ設定 • ログ管理 • ジョブ管理 • 証明書の管理	システム管理 • ドメインのセットアップ • ライセンス管理 • ユーザ管理 • **[LDAP Settings]** • **Cisco Prime Collaboration Assurance 12.1 Service Pack 3 の場合** セキュリティ設定 • シングル サインオン • バックアップ設定 • ログ管理 • ジョブ管理 • 証明書の管理
	UC オペレーション ダッシュボード • **UC オペレーション ダッシュボード** • レスポンダ設定
	サービサビリティ

Cisco Prime Collaboration Analytics の開始

Table 1 には、Cisco Prime Collaboration Analytics ダッシュボードの使用シナリオが示されています。

表 *8 : Cisco Prime Collaboration Analytics* ダッシュボードの開始

使用シナリオ	ダッシュレットの名前（分析からのナビゲーション）

音声専用の電話機、ビデオフォン、および TelePresence エンドポイントによる導入の進行状況を追跡します。	**Cisco Prime Collaboration リリース 11.1 以前の場合** エンドポイント モデルによる分配の導入（テクノロジの導入） **Cisco Prime Collaboration リリース 11.5 以降の場合** エンドポイント導入の概要（テクノロジの導入）
これまでの投資を検証し、将来の投資決定を行うためのエンドポイントの使用方法について理解します。	• **Cisco Prime Collaboration リリース 11.1 以前の場合** エンドポイント モデルによるコールの分配（テクノロジの導入） **Cisco Prime Collaboration リリース 11.5 以降の場合** エンドポイント モデルによるコール ボリューム（テクノロジの導入） • **Cisco Prime Collaboration リリース 11.1 以前の場合** エンドポイント タイプによるコールの分配（テクノロジの導入） **Cisco Prime Collaboration リリース 11.5 以降の場合** エンドポイント タイプによるコール ボリューム（テクノロジの導入）
使用頻度が高いまたは低いエンドポイントの数をカウントします。	テクノロジの使用（テクノロジの導入）
効果的に組織全体でリソースを計画および割り当てるために、使用頻度が最も低いエンドポイントを特定します。	使用頻度が最も低いエンドポイントタイプ（資産の使用率）
スケジュールされたセッションに参加しなかったエンドポイントを追跡します。	**Cisco Prime Collaboration Assurance 11.0 以前の場合** 不参加のビデオ会議（資産の使用率） **Cisco Prime Collaboration リリース 11.1 以降の場合** No Show Video TelePresence エンドポイント

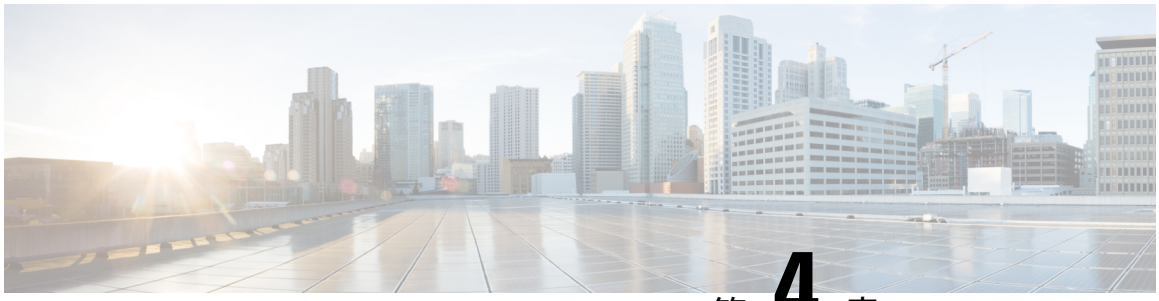
使用率が最も高いエンドポイントと最も低いエンドポイントを特定することができます。	ビデオ テレプレゼンス ルームの使用率（資産の使用率）
Cisco Prime Collaboration Assurance 管理による導入で、コールの最大発信回数または発信時間の順に並べ替えられた上位 N 個のディレクトリ番号を見つけます。	上位 N の発信者（トラフィック分析）
Cisco Prime Collaboration Assurance 管理による導入で、コールの最大受信回数または通話時間が最も長い順に並べ替えられた上位 N 個のディレクトリ番号を見つけます。	かけた番号の上位 N 位（トラフィック分析）
着信および発信オフネット コール数が最も高い拠点を検索します。	上位 N のオフネット トラフィック拠点（トラフィック分析）
発信および受信コール数が最も高い上位 N の拠点を特定します。	上位 N のコール トラフィック 拠点（トラフィック分析）
サイト、拠点、エンドポイント、クラスタ、デバイス プール間のさまざまなタイプのコールの傾向を把握します。	コール トラフィック分析（トラフィック分析）
組織全体にわたって使用を最適化するために、TelePresence 会議デバイスの使用状況を追跡します。	会議デバイスのビデオ使用率（キャパシティ分析）
失敗したコール数が最も高い拠点の Call Admission Control (CAC) 帯域幅使用率を考察することにより、各拠点に割り当てられる帯域幅を評価します。	拠点 CAC の帯域幅使用率（キャパシティ分析）
組織全体にわたって、トランクおよびルート グループの使用率を評価し、最適化します。また、カスタム トランクやルート グループの使用率を定義および追跡できます。	• トランク使用率（キャパシティ分析） • ルート グループの使用率（キャパシティ分析）
トランクとルート グループの Average Bouncing Busy Hour（ABBH）トラフィックを測定した後で、キャパシティ（回線）について決定します。	• 煩雑時のトランク キャパシティ（キャパシティ分析） • 煩雑時のルート キャパシティ（キャパシティ分析）
ゲートウェイの DSP リソースの最適化	DSP 使用率（キャパシティ分析）
組織内の個人が経験したサービス品質を分析します。	サービス エクスペリエンスの分配（サービス エクスペリエンス）

サービス品質問題が発生した上位 N のエンドポイントを指定します。	**Cisco Prime Collaboration リリース 11.1 以前の場合** サービス品質に問題があるエンドポイント（サービス エクスペリエンス） **Cisco Prime Collaboration リリース 11.5 以降の場合** コール品質に問題があるエンドポイント（サービス エクスペリエンス）
組織内のコールの失敗の傾向を分析し、コール失敗発生率が高い拠点を特定します。	上位 N のコール失敗発生拠点（サービス エクスペリエンス）
サービス品質問題があるユーザを識別します。	サービス品質問題があるユーザ（サービス エクスペリエンス）
組織の UC アプリケーションのシステム パフォーマンスを分析します。	UC システム パフォーマンス
会議の統計情報の視覚化（会議の数と期間）	• ビデオ会議の統計（ビデオ会議） • 上位 N のビデオ会議の拠点（ビデオ会議）

第 II 部

サーバのセットアップ

- サードパーティ CA 署名付き証明書の有効化 （63 ページ）
- ライセンスの管理 （67 ページ）
- [ユーザ管理（Manage Users）] （75 ページ）
- 顧客の管理 （87 ページ）
- ドメインの管理 （89 ページ）
- システム パラメータの設定 （91 ページ）



第 4 章

サードパーティ CA 署名付き証明書の有効化

このセクションでは、次の点について説明します。

- サードパーティ CA 署名付き証明書の有効化 （63 ページ）

サードパーティ CA 署名付き証明書の有効化

セキュアなデータ転送のために、自分の会社の署名付き証明書をインポートすることができます。この証明書を使用するブラウザで、SSL を有効にする必要があります。

CA 署名付き証明書のインストール

セキュアなデータ転送のための CA 署名付き証明書のインストール：

始める前に

セキュリティを強化し、管理を容易にし、証明書管理を実践するために、情報資産を保護する目的で、次の要素が検証されます。

Cisco Prime Collaboration リリース 12.1 SP3 以降の場合

CA の署名付き証明書は、次の要件のリストを満たしている必要があります。要件：

- "Primecollab" エイリアスを含む。
- 正しいパスワードを使用してインポートできる。
- 30 年以上にわたって有効な状態を維持する。
- 有効期限が設定されている。有効期限が
  - 切れていないこと

    例：現在の日付が 20/9/2019 の場合、有効期間（20/8/1970-20/8/2000）は無効です。
  - 将来の日付に設定されていないこと

例：現在の日付が 20/9/2019 の場合、有効期間（20/12/2020-20/12/2025）は無効です。

- 「有効なサンプル」有効期間

  例：現在の日付が 20/9/2019 の場合、有効期間（20/9/2019-20/9/2025）は有効です。

- 証明書に指定する CN（共通名）または SAN（サブジェクトの別名）が、PCA サーバの FQDN（完全修飾ドメイン名）と一致する必要があります。
  - PCA サーバの FQDN が CN と一致しない場合は、SAN のリストと照合されます。
  - ユーザは、CN に FQDN を使用して CSR（証明書署名要求）を生成するか、または SAN のリストに FQDN を含める必要があります。例：pcatest.cisco.com（FQDN）。
- 署名アルゴリズムが、TBSCertificate シーケンスに存在する署名アルゴリズム ID と一致する必要があります。
- 拡張を重複させることはできません。
- サポート対象外の重要な拡張は使用できません。
  - チェックは、重要としてマークされている拡張のみに適用されます。
  - サポート対される拡張は、BC（BasicConstraints）、KU（KeyUsage）、EKU（ExtendedkeyUsage）、SAN（SubjectAlternativeName）、IAN（IssuerAlternativeName）、SIA（SubjectInfoAccess）、AIA（AuthorityInfoAccess）です。
- 重要な KeyUsage（KU）があり、有効であること
  - KU 拡張が重要としてマークされていれば、チェックが適用されます。
  - 有効な KU は keyCertSign、cRLSign、digitalSignature です。
- 重要な ExtendedKeyUsage（EKU）があり、有効であること。
  - EKU 拡張が重要としてマークされていれば、チェックが適用されます。
  - 有効な EKU は serverAuth、clientAuth、OCSPSigning です。

上記の要件を 1 つでも満たしていない場合、証明書は拒否され、該当するエラーメッセージによってユーザにアラートが送られます。

Cisco Prime Collaboration リリース 11.5 以降の場合

- ルート証明書が、署名付き証明書に含まれている。
- SSL がブラウザで有効であり、CA 署名付き証明書を使用できる。

ステップ 1 選択 **[システム管理（System Administration）] > [証明書の管理（Certificate Management）] > [Cisco Prime Collaboration 証明書の管理（Cisco Prime Collaboration Certificate Management]**.

ステップ 2 ローカル システムから、（PKCS12 形式の）CA 署名付き証明書を参照します。

ステップ 3 （任意）証明書の生成中にパスワードを設定した場合は、PKCS#12 ファイルの証明書のパスワードを入力して確認します。設定していない場合は、入力する必要はありません。

ステップ 4 [インポート（Import）] をクリックします。

「サービスが再起動されます」という内容の警告メッセージが表示されます。

ステップ 5 警告メッセージが表示されたら、[Continue] をクリックします。
証明書がサーバにインポートされます。

（注） 証明書をインポートした後は、Cisco Prime Collaboration Assurance を手動で再起動する必要があります。

Cisco Prime Collaboration リリース 12.1 SP3 以降の場合

Cisco Prime Collaboration Assurance サーバを再起動するには、*root* としてログインし、次のコマンドを実行します。

1。プロセスを停止します。

「root@<hostname>~#/opt/emms/emsam/bin/cpcmcontrol.sh stop」

2。プロセスのステータスを確認します。 - Verify whether the processes have stopped:

「root@<hostname>~#/opt/emms/emsam/bin/cpcmcontrol.sh status」

3。プロセスを再起動します。

「root@<hostname>~#/opt/emms/emsam/bin/cpcmcontrol.sh start」

サービス再起動後、ログインページが表示されます。セキュリティ警告ページ（ログインページが表示されるよう選択を行うページ）は、これ以降表示されません。

（注） Cisco Prime Collaboration Assurance サーバを起動する前に、プライマリおよびセカンダリの中間証明書をブラウザへインポートしておくことをお勧めします。これにより、CA 署名付き証明書をインストールした後、最初にサーバを起動したときに、接続がプライベートでないという警告が表示されないようになります。

PKCS12 証明書は、どのエイリアス名でもインポートできます。

PEM/DER 形式（.pem、.cer、.der、.key など）はサポートされないため、KCS#12 形式（.pfx または .p12）の証明書を使用する必要があります。

Cisco Prime Collaboration リリース 11.6 以降の場合

（注） PKCS12（.pfx または .p12）形式の署名付き証明書がインポートされていることを確認してください。

証明書には、**primecollab** エイリアスが含まれている必要があります。

primecollab エイリアスのキーのパスワードは、証明書のパスワードと同じである必要があります。

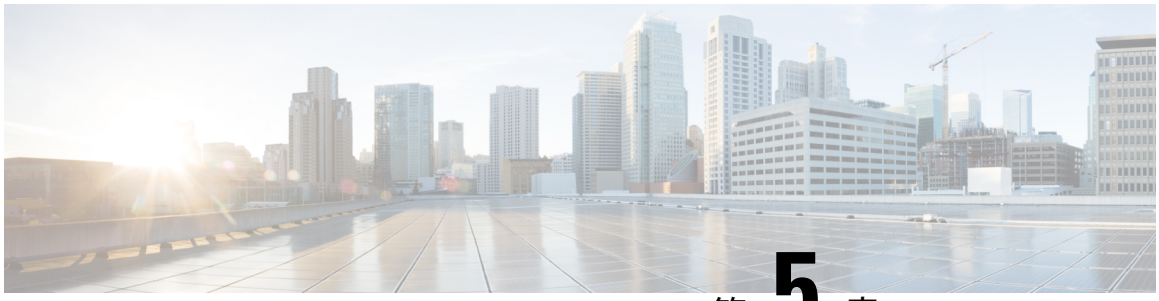
Cisco Prime Collaboration リリース 12.1 以降の場合

PKCS7 または PKCS12 の証明書を適用したバージョン 11.x の Cisco Prime Collaboration Assurance を、バージョン 12.1 に移行すると、証明書が復元されません。Cisco Prime Collaboration Assurance 12.1 用に証明書を再生成する必要があります。

（注） Cisco Prime Collaboration Assurance 11.6 以降では、PKCS12 の証明書のみがサポートされています。

プライマリ/中間/セカンダリの証明書をブラウザへインポートするには、次の表を参照してください。

ブラウザ	操作
Internet Explorer	選択 **[ツール（Tools）]** > **[インターネット オプション（Internet Options）]**> **[コンテンツ（Content）]**> **[証明書（Certificates）]**> **[信頼されたルート証明機関（Trusted root certification authorities）]** > **[インポート（Import）]**
Mozilla Firefox	選択 **[ツール（Tools）]** > **[オプション（Options）]**> **[拡張機能（Advanced）]**> **[証明書（Certificates）]**> **[証明書を表示（View certificates）]** > **[インポート（Import）]**
Chrome	選択 **[設定（Settings）]** > **[詳細設定（Advanced settings）]** > **[HTTP/SSL証明書の管理（ HTTP/SSL Manage certificates）]**> **[信頼されたルート証明機関（Trusted root certification authorities）]**> **[インポート（Import）]**



第 5 章

ライセンスの管理

このセクションでは、次の点について説明します。

- ライセンスの管理 （67 ページ）

ライセンスの管理

Cisco Prime Collaboration Assurance ライセンスにより、インストールする Cisco Prime Collaboration Assurance アプリケーションのエンドポイント数を有効にできます。エンドポイントの数量に基づいてライセンスを注文することができます。Cisco Prime Collaboration Assurance および Prime Collaboration Provisioning両方次のページに移動します。 **[システム管理（System Administration）] > [ライセンス管理（License Management）]**。

Cisco Prime Collaboration Assurance を Advanced モードのいずれかでインストールできます。

評価モードで追加できるエンドポイントの数は、Assurance の OVA サイズによって異なります。Cisco Prime Collaboration Assurance によって、インベントリに追加したデバイスの数が記録されます。追加可能なデバイスの数が、デバイス許容数に近づくと、警告メッセージが表示されます。システム インベントリで、OVA をアップグレードするか、既存のデバイスをいくつか削除できます。

Cisco Prime Collaboration Assurance の評価期間は 60 日です。評価期間後は、ログインするたびに Assurance によって [ライセンス管理（License Management）] ページにリダイレクトされます。

（注） 「スマート ライセンス」は、Cisco Prime Collaboration Assurance リリース 12.1 でサポートされていません。

Cisco Prime Collaboration Assurance のライセンシング

Cisco Prime Collaboration Assurance ライセンスは、エンドポイントの数量に基づいています。エンドポイント数は、ネットワークを管理するために購入の必要があるライセンス数を決定します。

Cisco Prime Collaboration Assurance は、**[ライセンス管理（License Management）]**次のページで合計エンドポイントのライセンス状態を提供します。**[システム管理（System Administration）]**> **[ライセンス管理（License Management）]**。

（注） ソフト フォンが、ハード フォンと同じようにライセンスを消費します。すべてのソフト フォンは、Unified CM に登録されたハード フォンと同じディレクトリ番号を共有している場合でも、1 つのライセンスが必要です。

これらのエンドポイントの詳細については、『Cisco Prime Collaboration Assurance および Analytics のインストールとアップグレード ガイド』を参照してください。

Cisco Prime Collaboration Analytics ライセンス

Cisco Prime Collaboration Analytics ライセンスは、必ず Cisco Prime Collaboration Assurance ライセンスの導入後または導入時に適用する必要があります。

Cisco Prime Collaboration リリース 11.1 以前の場合

Cisco Prime Collaboration Analytics 機能にアクセスするには、Enterprise モードで Cisco Prime Collaboration Assurance を導入する必要があります。Cisco Prime Collaboration Analytics は、Managed Service Provider（MSP）モードではサポートされていません。

評価モード（60 日）後に Cisco Prime Collaboration Analytics ダッシュボードにアクセスするには、Cisco Prime Collaboration Analytics のライセンスを購入する必要があります。Cisco Prime Collaboration Assurance と同じスケール ライセンスを購入する必要があります。Cisco Prime Collaboration Assurance のライセンスを Advanced モードで追加した後でも、引き続き評価モードで Cisco Prime Collaboration Analytics にアクセスできます。

Analytics ライセンス ファイルを追加するには、次のオプションを選択します。 **[システム管理（System Administration）]** > **[ライセンス管理（License Management）]**。

Analytics ライセンスの追加

Cisco Prime Collaboration Analytics ライセンスは、アシュアランスの合計と同数またはそれ以上にする必要があります。

評価モードでは、Cisco Prime Collaboration Analytics のライセンスは Cisco Prime Collaboration Assurance のライセンスと同じです。

Analytics ライセンス ファイルを追加するには、次のオプションを選択します。 **[システム管理（System Administration）]** > **[ライセンス管理（License Management）]**。

Cisco Prime Collaboration Analytics の NFR ライセンスの購入は、Cisco Prime Collaboration Assurance ライセンスの購入後にのみ可能になります。

Analytics の有効化と無効化

始める前に

Analytics の機能を有効または無効にするには、Cisco Prime Collaboration Analytics を評価モードにしておく必要があります。

ステップ 1 選択 **[システム管理（System Administration）] > [ライセンス管理（License Management）]**。

ステップ 2 Cisco Prime Collaboration Assurance および Analytics の非常に大きい OVA を導入した場合は、リモート Cisco Prime Collaboration Analytics データベースを導入した後で次の手順を実行してください。

a) [Analytics] ペインで [Setup Remote Analytics DB] をクリックし、リモート Cisco Prime Collaboration Analytics データベースを設定します。

b) リモート データベースの IP アドレスを入力して [OK] をクリックします。

ステップ 3 [Analytics] ペインで [Enable Analytics] をクリックしてデータ分析を有効にします。

ステップ 4 ブラウザからログアウトし、Cisco Prime Collaboration Assurance Serviceability User Interface にログインします。

ステップ 5 [Dashboard] をクリックします。

ステータスとシステムの更新履歴のほか、すべてのプロセスを表示できます。すべてのプロセスを開始および停止することができます。

ステップ 6 Cisco Prime Collaboration Assurance サーバにログインし、Analytics のライセンスがアクティブかどうかを確認します(**[システム管理（System Administration）] > [ライセンス管理（License Management）]**。

Analytics を無効にする場合は、[Analytics] ペインで [Disable Analytics] をクリックします。無効にした後で、アプリケーションおよびデータベース（非常に大きい OVA の場合のみ）サーバ上のプロセスを再起動する必要があります。分析されたすべてのデータが消去され、[Analyze] タブが無効になります。

Cisco Prime Collaboration Contact Center Assurance のライセンス

Cisco Prime Collaboration Contact Center Assurance は、Cisco Prime Collaboration Assurance Advanced 展開でのみサポートされます。Cisco Prime Collaboration Contact Center Assurance ライセンスは、Unified Contact Center Enterprise（Unified CCE）に同時にログインしているエージェント数に基づきます。Cisco Prime Collaboration Contact Center Assurance ライセンスの適用は、Cisco Prime Collaboration Assurance Advanced ライセンスを追加した後に行う必要があります。

Cisco Prime Collaboration Assurance は、Unified Contact Center Enterprise にログインしているエージェント数を 30 分ごとにポーリングします。ログイン中のエージェント数がライセンス ファイルに記載されている許可数を超えると、システムから警告が表示されます。

受信した警告の数がいくつでも、Cisco Prime Collaboration Assurance で生成される違反は 1 日に 1 つです。30 日以内にこのような違反が 10 個出された場合、10 回目の違反を受信した時点から 30 日以内にライセンスが有効期限切れになります。

ライセンス ファイルを Cisco Prime Collaboration Assurance Advanced に追加して Cisco Prime Collaboration Contact Center Assurance に追加しなかった場合、Cisco Prime Collaboration Contact Center Assurance の機能には、ライセンスを購入しない限り評価期限までしかアクセスできません。

ライセンスが期限切れになると、Unified Contact Center のインフラストラクチャ デバイスは、UC パフォーマンス ダッシュボード、[しきい値ルール（Threshold Rules）] ウィンドウ、および[相関ルール（Correlation Rules）] ウィンドウに表示されなくなります。SIP Call Flow Analyzer では、Contact Center デバイス（Unified CCE、CVP）やその他の UC コンポーネントから受信したコール ログを分析できなくなります。Contact Center トポロジ全体のビューも使用できなくなります。

これらの機能を引き続き使用するには、必要な数の Cisco Prime Collaboration Contact Center の同時エージェント ライセンスを購入する必要があります。Cisco Prime Collaboration Contact Center Assurance のライセンスの詳細を表示するには、**[システム管理（System Administration）]** > **[ライセンス管理（License Management）]** ページで設定しなければならない場合があります。

Cisco Prime Collaboration Contact Center Assurance ライセンスの追加後に拡張される機能の詳細については、『Cisco Prime Collaboration Contact Center Assurance ガイド』を参照してください。

ライセンスの購入後に管理できるエージェントの数は、Evaluation モードの場合と変わりません。詳細については、『Cisco Prime Collaboration Assurance and Analytics インストールおよびアップグレード ガイド』の「エンドポイントとコンタクト センター エージェントの数」の項を参照してください。

[ライセンスのカウント（License Count）]

Cisco Prime Collaboration リリース 12.1 以降の場合

エンドポイント ライセンシングは 15 分ごとに実行されます。ライセンス基準に従い、管理されたエンドポイントの合計数が購入したライセンス数を超えることはありません。

- ライセンス基準を満たさない場合、エンドポイントは削除されます。最初に、未登録のエンドポイントが削除されます。
- それでもライセンス基準を満たさない場合、登録済みのエンドポイントが削除されます。

デバイスの検出と管理の詳細については、デバイスの検出を参照してください。追加されていないエンドポイントが検出ジョブにリストされます。

Cisco Prime Collaboration Assurance を MSP モードで導入した場合、IP アドレスが重複する電話機は、異なるエンドポイントとしてカウントされます。

Cisco Prime Collaboration Assurance のおよびエンドポイント数

次の電話機が、Cisco Prime Collaboration Assurance にカウントされています。

- ソフト クライアントには、Cisco Unified Personal Communicator、Cisco IP Communicator、Cisco Jabber、Client Services Framework（CSF）があります。

- 携帯電話は別にカウントされます。
- 音声ゲートウェイに接続しているアナログ電話は監視されないため、カウントされません。

（注） システムは各エンドポイントをカウントし、Jabber と IP フォンは別々にカウントされます。

ライセンス詳細の表示

[ライセンス管理（License Management）]ページ（**[システム管理（System Administration）]**> **[ライセンス管理（License Management）]**の順に移動）では、次の Cisco Prime Collaboration Assurance ライセンス情報が表示されます。

Cisco Prime Collaboration リリース 11.6 以降の場合

システム情報

- MAC アドレス
- DB サーバ IP アドレス

（注） [DB サーバ IP アドレス（DB server IP Address）] フィールドは、Cisco Prime Collaboration Assurance の特大 OVA 導入モデル固有のものであり、小、中、大の OVA 導入モデル の [Assurance 情報（Assurance Information）] リンクには表示されません。

Cisco Prime Collaboration リリース 12.1 以降の場合

これは、3 種類のライセンス タイプ（Assurance、Analytics、Contact Center Assurance）であることを意味します。

（注） また、各ライセンス タイプ（アシュアランス、分析、Contact Center Assurance）に割り当てられたライセンス数を追跡することもできます。

ライセンス ファイルをアップロードすると、ライセンス数が表示されてプロファイルごとのカウント数を確認でき、これが最大数を超えると、最大数が超えたことを示す警告メッセージが表示されます。メッセージは、ライセンス モードに固有のものです。

（注） [アシュアランス（Assurance）] および [分析（analytics）] モードに固有の一般的な警告メッセージ、ならびに Contact Center Assurance モードに固有のメッセージを 1 つ受け取ります。

Assurance ライセンス ステータス

- インストール済みのアクティブなベース ライセンス - 評価またはイメージです。
- 使用済みの合計エンドポイント ライセンス数 - 使用可能な合計ライセンス数と現在使用中のライセンス数です。Advanced モードの合計ライセンス数の詳細については、「「ライセンス数」」セクションを参照してください。
- ライセンスの有効期限 - ライセンスの有効期限が切れる日付です。この値は、Evaluation ライセンスのみに適用されます。

（注） 評価期限が過ぎた後でライセンスを取得すると、[License Expiration Date] の値は **[Permanent]** に変わります。

- インストール済みの合計エンドポイント ライセンス数 - インストール済みの合計ライセンス数です。

Analytics および Contact Center Assurance のライセンシングでは、次の情報が表示されます。

Enterprise モード	**マネージド サービス プロバイダー（MSP）モード**
分析： • インストールされているライセンス • ライセンスの有効期限	**Cisco Prime Collaboration リリース 11.5 以降の場合** 分析： • インストールされているライセンス • ライセンスの有効期限
Contact Center Assurance： • インストールされているライセンス • ライセンスの有効期限	Contact Center Assurance： • インストールされているライセンス • ライセンスの有効期限

（注） Contact Center Assurance のライセンシングのライセンス有効期限は、ユーザ インターフェイスにおける Assurance のライセンス ステータスと同じですが、Contact Center Assurance のライセンスの有効期限は、同時にログインする Unified CCE エージェントの数によって変わることがあります。

Cisco Prime Collaboration Assurance にライセンスを登録してライセンス ファイルを取得するには、および『Cisco Prime Collaboration Assurance および Analytics のインストールとアップグレード ガイド』を確認する必要があります。

ライセンス ファイルの追加と削除

実稼働ネットワークでCisco Prime Collaboration Assurance アプリケーションをアクティブ化する場合は、Cisco Prime Collaboration Assurance 任意の数のスケール ライセンスを追加できますが、Cisco Prime Collaboration Assurance に対して、イメージ ライセンス ファイルは 1 回追加され、個別に追加されます。

Cisco Prime Collaboration Assurance にライセンス ファイルを追加するには、次のようにします。

ステップ 1 選択 **[システム管理（System Administration）] > [ライセンス管理（License Management）]**。
[License Management] ページが表示されます。

ステップ 2 [ライセンスファイル（License Files）] の下で [追加（Add）] をクリックします。
[Add License File] ポップアップ ページが表示されます。

ステップ 3 [Browse] をクリックしてライセンス ファイルをアップロードして [OK] をクリックします。
新しく追加されたライセンス ファイル情報は、Cisco Prime Collaboration Assurance の [License Status] ペインに表示されます。

（注） ライセンス ファイルを削除するには、**[システム管理（System Administration）] > [ライセンス管理（License Management）]** を選択します。**[ライセンス管理（License Management）]** ページでライセンス ファイルを選択し、**[削除（Delete）]**をクリックします。

評価モードから実稼働にアップグレードする場合は、デバイスの再検出を実行します。デバイスの再検出については、デバイスの再検出 （168 ページ）

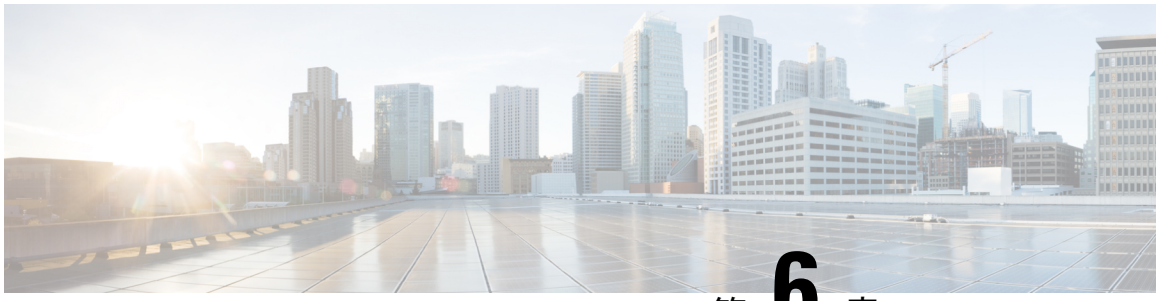
Cisco Prime Collaboration Assurance で Advanced Evaluation から Advanced（有料ライセンス）に切り替える

Cisco Prime Collaboration Assurance では、Advanced Evaluation から Advanced（有料ライセンス）に切り替えることができます。

次の表には、切り替え時のさまざまなシナリオが示されています。

表 9 : Cisco Prime Collaboration Assurance で Advanced Evaluation から Advanced（有料ライセンス）に切り替える

インストール モード	**Advanced Evaluation から Advanced（ライセンスを購入）**
Cisco Prime Collaboration Assurance	はい。（ユーザ インターフェイスの右上にある **[Get Advanced]** アイコン⬆をクリックして **[Add Licenses]** をクリックします）[License Management] ページで、**[Add]** をクリックし、Advanced モードのライセンス ファイルをアップロードします。）



第 6 章

[ユーザ管理（Manage Users）]

このセクションでは、次の点について説明します。

- [ユーザ管理（Manage Users）]（75 ページ）

[ユーザ管理（Manage Users）]

Cisco Prime Collaboration Assurance は、さまざまなタスクを実行できるようにする事前定義済みのアクセス コントロールを持つ、組み込みの静的ロールをサポートしています。

Cisco Prime Collaboration Assurance では、ユーザを作成し、ユーザにロールを割り当てることができます。

Cisco Prime Collaboration Assurance では、こうした組み込みの静的ロールによって、ロールベース アクセス コントロール（RBAC）が有効化されます。したがって、ユーザが実行できるタスク、またはユーザが表示または管理できるデバイスまたはデバイス グループは、ネットワーク管理者が割り当てたロールによって制御されます。

デバイスまたはデバイス グループをドメイン（Cisco Prime Collaboration Assurance を Enterprise モードで導入している場合）に関連付けることにより、選択したデバイスまたはデバイス グループ、およびそれらに関連するタスクのアクセス制御を強化できます。通常、オペレータ ロールを持つユーザは、特定の ドメインにのみアクセスが許可されます。

Cisco Prime Collaboration Assurance - 高度なユーザ ロール

ユーザ ロールは、ユーザがアクセスできるタスクの許可を定義するために使用されます。

次のロールのいずれかを割り当てることができます。

- **Cisco Prime Collaboration リリース 11.5 以降の場合**

  レポート ビューア：レポートを表示およびエクスポートすることのみ可能です。レポート ビューアのホームページは、CDR および CMR レポートです。レポート ビューアのユーザ ロールでは、**検索**、**デバイス ス テータスの概要**、**アラーム**、**Advanced を取得**などのグローバル ユーザ インターフェイス コンポーネントを使用することはできません。次のものを除き、すべてのレポートを表示できます。

- CUCM レポートの起動
- 管理レポート
- スケジュール済みレポート

- ヘルプデスク：ネットワーク ステータス情報の表示とアクセスのみが可能です。また、デバイスでアクションを何も実行できず、ネットワークに到達するジョブをスケジュールすることもできません。
- オペレータ：すべてのヘルプデスク タスク、およびネットワーク データの収集に関連するタスクを実行します。デバイスの追加、検出、またはインポートなどのインベントリ管理操作は実行できません。また、アラームとイベントのしきい値を設定することもできません。
- ネットワーク管理者：すべてのオペレータ タスクと、クレデンシャルの管理やしきい値の設定など、ネットワーク設定の変更を引き起こすタスクを実行します。
- システム管理者：バックアップと復元、ログ ファイルの保守、ユーザの設定など、Assurance のユーザ インターフェイス関連の管理タスクを実行します。
- スーパー管理者：システム管理者とネットワーク管理者の両方が実行できるタスクを実行します。

ヘルプデスクは、Cisco Prime Collaboration Assurance のすべてのユーザに対して事前に割り当てられるロールです。

Cisco Prime Collaboration リリース 11.5 以降の場合

レポート ビューアは、Cisco Prime Collaboration Assurance のすべてのユーザに対して事前に割り当てられるロールです。

ユーザに対して選択されたロールによって、他のユーザのデータに対するアクセス権が決まります。たとえば、スーパー管理者のロールを持つユーザは、他のすべてのユーザを表示できますが、ネットワーク管理者のロールを持つユーザは、スーパー管理者やシステム管理者などの上位のロールを持つユーザを表示することはできず、オペレータやヘルプデスクのロールを持つ他のユーザのデータは参照できます。

Cisco Prime Collaboration Assurance を MSP モードで展開した場合は、同じロールを持つ別のユーザに属する顧客を（その顧客に関連付けられているユーザであれば）参照することができます。

Cisco Prime Collaboration Assurance を ENT モードで展開した場合は、同じロールを持つ別のユーザに属するドメインを（そのドメインに関連付けられているユーザであれば）参照することができます。

注記：[ユーザ管理（User Management）] サブメニューは、次のロールでは使用できません。

Cisco Prime Collaboration リリース 11.5 以降の場合

1. Report Viewer
2. Helpdesk

3. 演算子

Cisco Prime Collaboration リリース 11.6 以降の場合

デフォルトのユーザ ロールの選択は、Cisco Prime Collaboration Assurance から削除されています。

（注） レポート ビューアのロールが選択されたユーザが他のロールを選択することや、他のロールのユーザがレポート ビューアを選択することはできません。

Cisco Prime Collaboration リリース 12.1 SP3 以降の場合

複数レベルでの承認を可能にするために、次のロールがサポートされています。

1. **ネットワーク管理者**：すべてのオペレータ タスクと、クレデンシャルの管理などのネットワーク設定の変更を引き起こすタスクを実行します。
2. **システム管理者**：ユーザ インターフェイス関連の管理タスクを実行します。
3. **スーパー管理者**：システム管理者とネットワーク管理者の両方が実行できるタスクを実行します。

関連トピック

顧客の管理 （87 ページ）
ドメインの管理 （89 ページ）

Cisco Prime Collaboration Assurance のシングル サインオン

Cisco Prime Collaboration Assurance はセキュリティ アサーション マークアップ言語（SAML）を使用して Cisco Prime Collaboration Assurance でのシングル サインオン（SSO）を可能にする管理者権限をユーザに提供します。

Cisco Prime Collaboration Assurance は、マルチサーバの SAN 証明書およびエンドユーザの SAML SSO をサポートしていません。

SSO を有効にする前に、次の前提条件が満たされていることを確認してください。

- Cisco Prime Collaboration Assurance で LDAP 管理ユーザを手動で作成することにより、システムには少なくとも 1 人の LDAP 管理ユーザが存在します。
- Identity Provider（IdP）サーバは、単一ホストのアプリケーションおよびサービス プロバイダーが提供するその他多くのアプリケーションへのアクセスに SSO を使用できるようにします。サービス プロバイダーとはアプリケーションをホストする Web サイトです。

  次に、サポートされているサードパーティ IdP サーバを示します。

  - Open Access Manager（OpenAM）
  - Ping ID
  - Active Directory Federation Services（ADFS）
  - Oracle Identity Manager

IdP サーバをセットアップする手順については、『SAML SSO Deployment Guide for Cisco Unified Communication Applications, Release 10.0(1)』を参照してください。

- IdP サーバからのアイデンティティ プロバイダーのメタデータ ファイルをダウンロードし、ローカル システムに保存します。

シングル サインオンを有効にするには、次の手順を実行します。

ステップ 1 選択 **[システム管理（System Administration）] > [シングル サインオン（Single Sign-On）]**。

ステップ 2 [SSO を有効にする（Enable SSO）] をクリックします。

「Enabling SSO redirects you to the IdP server for authentication from the next login」という警告メッセージが表示されます。アプリケーションにアクセスするには、正常に認証される必要があります。

（注） 前述の前提条件が満たされていない場合は、[SSOを有効にする（Enable SSO）] は無効になっています。

ステップ 3 [続行（Continue）] をクリックします。

ステップ 4 シングル サインオンを有効にするには、SSO ウィザードに示される手順に従います。

a) ローカル システムから IdP メタデータ ファイルを見つけ、[IdP メタデータのインポート（Import IdP Metadata）] をクリックします。

b) [Trust Metadata ファイルのダウンロード（Download Trust Metadata file）] をクリックします。

c) IdP サーバを起動し、ダウンロードした信頼メタデータ ファイルをインポートします。

（注） これは、SSO を有効にするための手動の手順です。SSO のテストを進める前に、IdP サーバで信頼範囲（CoT）を作成し、ログアウトする必要があります。

d) SSO のテスト セットアップを実行するには、[有効な管理ユーザ名（Administrative Usernames）] ドロップダウンからユーザ名を選択します。Active Directory の管理者であり、SSO ユーザの下で Cisco Unified CDM によって同期される任意のユーザを入力することができます

（注） ほかのユーザ名を使用して IdP サーバにログインすると、管理者アカウントがロックされる可能性があります。

e) [SSOテストの実行（Run SSO Test）] をクリックし、IdP サーバ、Cisco Prime Collaboration Assurance のアプリケーション、シングル サインオン間の接続をテストします。

「Unable to do Single Sign-On or Federation」というエラー メッセージが表示された場合は、次の手順を実行します。

- エンド ユーザ クレデンシャルを使用して手動で IdP サーバにログインし、認証が成功したかどうかを確認します。
- Trust Metadata ファイルが IdP サーバで正常にアップロードされているかどうかを確認します。
- Cisco Prime Collaboration Assurance サーバと IdP サーバが同じ信頼の輪にあるかどうかを確認します。

f) [終了（Finish）] をクリックします。

SSO のトラブルシューティングおよびログ

- SSO を有効化している間に Cisco Prime Collaboration Assurance サーバからログアウトした場合は、ブラウザを閉じて、Cisco Prime Collaboration Assurance アプリケーションを再起動することを推奨します。これは、Cisco Prime Collaboration Assurance サーバでの会議が期限切れになっても、IdP サーバ 会議はまだアクティブである可能性があるためです。
- SSO を有効化中、Cisco Prime Collaboration Assurance のホスト名が設定され、DNS の一部であることを確認します。

IdP サーバがダウンしている場合は、次のことが可能です。

- リカバリ URL（https://<PCserver IP アドレス または DNS に含まれているホスト名>:8443/ssosp/local/login）を使用します。
- CMD ユーティリティからシングル サインオンを無効にします。

Cisco Prime Collaboration Assurance アプリケーションで CMD ユーティリティから SSO を無効化するには、以下を実施します。

- ポート 26 の SSH を使用して Cisco Prime Collaboration Assurance サーバにログインします。
- Cisco Prime Collaboration Assurance の **/opt/emms/emsam/bin** ディレクトリに移動します。次の表に基づいて、**cpcmconfigsso.sh** ファイルの <Operation> と <Value> のエントリを追加します。

操作は次のとおりです。	値は次のとおりです。
1：シングル サインオン ステータスを取得	N/A
2：リカバリ URL ステータスを取得	N/A
3：シングル サインオン ステータスを設定	False （注） CLI から SSO を有効にすることはできません。SSO を有効にするにはユーザ インターフェイスの手順を使用します。
4：リカバリ URL ステータスを設定	True または False

- SSO を無効にするには、次のコマンドを実行します。

cpcmconfigsso.sh 3 false

（注） リカバリ URL は有効になっています。セキュリティ上の理由でこれを無効にする場合は、デフォルトで False に設定します。

デフォルト ユーザ アカウント

というデフォルトの Web クライアント管理者ユーザで事前設定されます。globaladmin は、の両方にアクセスできるスーパーユーザです。

仮想アプライアンスを設定するときに、globaladmin のパスワードを指定します。このクレデンシャルは、Cisco Prime Collaboration Assurance の Web クライアントを初めて起動する際に必要です。

注意 パスワードを忘れたり紛失した場合のために、root パスワードを書き留めておくことをお勧めします。root パスワードをリセットするには TAC サポート ケースを開く必要があります。

Cisco Prime Collaboration Assurance の Web クライアントに初めてログインする場合は、*globaladmin* としてログインします。

（注） これらのユーザのパスワード検証ルールについては、『Cisco Prime Collaboration Assurance および Analytics のインストールおよびアップグレード ガイド』を参照してください。

注意 名前を使用してユーザを作成しないでください（globaladmin、pmadmin、および admin）。

選択 。[ログをダウンロード（Download Log）] ボタンをクリックします。tar ファイルをダウンロードし、untar します。/opt/emms/emsam/log/importedprovisioninguser.log ファイルを確認し、重複するユーザ名（すでにCisco Prime Collaboration Assurance で使用されているユーザ名）、ユーザ名にパスワードがないなどの理由で Cisco Prime Collaboration Assurance データベースにインポートされなかったユーザを検索します。

Cisco Prime Collaboration Assurance アプリケーションは、互いにインベントリ データベースを共有しません。のタスクを実行するには、デバイスを別々に管理する必要があります。Cisco Prime Collaboration Assurance アプリケーションを使用してデバイスの管理タスクを実行するには、「デバイス クレデンシャルの管理 （99 ページ）」を参照してください。

関連トピック

デバイス クレデンシャルの管理
デバイス グループの管理 （173 ページ）

ユーザ ロールおよびタスク

Cisco Prime Collaboration Assurance バージョン 11.x の [ユーザ ロールおよびタスク（User Roles and Tasks）と、Cisco Prime Collaboration Assurance バージョン 12.x の [ユーザ ロールおよびタスク（User Roles and Tasks）]には、自身に対応付けられた Cisco Prime Collaboration Assurance のロールおよびタスクが一覧で表示されます。

（注） スーパー管理者は、すべてのユーザ インターフェイス メニューにアクセスし、すべてのタスクを実行できます。したがって、スーパー管理者は一覧に表示されません。

関連トピック

Cisco Prime Collaboration Assurance のユーザ ロールとタスク

ユーザの追加

ユーザを追加して、事前定義済みの静的ロールを割り当てることができます。ユーザは、Cisco Prime Collaboration Assurance の Web クライアントにのみアクセスでき、Cisco Prime Collaboration Assurance サーバに CLI からログインすることはできません。

ユーザを追加するには、次の手順を実行します。

ステップ 1 選択 **[システム管理（System Administration）]** > **[ユーザ管理（User Management）]**。

ステップ 2 **[ユーザ管理（User Management）]** ページで、**[追加（Add）]** をクリックします。

ステップ 3 **[ユーザの追加（Add User）]** ページで、必要なユーザの詳細情報を入力します。

LDAP サーバは認証を実行するため、Cisco Prime Collaboration Assurance と同じユーザ ID を持っている必要があることに注意してください。詳細については、「LDAP サーバの設定」を参照してください。

[LDAP User] オプションを選択した場合、[Password] フィールドおよび [Confirm Password] フィールドは表示されません。

ステップ 4 適切な Cisco Prime Collaboration Assurance ロールを選択します。

ステップ 5 **[Save]** をクリックします。

ユーザの詳細を編集するには、**[システム管理（System Administration）]** > **[ユーザ管理（User Management）]** を選択して、必要な変更を行います。

Cisco Prime Collaboration リリース 11.6 以降の場合

レポート ビューアーのユーザ ロールを割り当て済みのロールから除外するには、[レポートビューアー（Report Viewer）] オプションを手動で選択解除して [保存（Save）] をクリックします。

通常のシステム管理タスクの一部として、Cisco Prime Collaboration Assurance データベースからユーザを削除する必要がある場合があります。ただし、Cisco Prime Collaboration Assurance の Web クライアントのデフォルトの管理者である *globaladmin* は削除できません。

ユーザを削除するには、**[システム管理（System Administration）]** > **[ユーザ管理（User Management）]** **[削除（Delete）]**をクリックします。削除したユーザ名でスケジュールされたジョブは、キャンセルされるまで引き続き実行されます。

ユーザ ロールの変更

ユーザの連絡先情報、ロール、またはアカウント ステータスが変更された場合、管理者はシステムの対応する情報を編集する必要があります。

ユーザの詳細を編集するには、**[システム管理（System Administration）]**>**[ユーザ管理（User Management）]** を選択して、必要な変更を行います。

Cisco Prime Collaboration リリース 11.6 以降の場合

レポート ビューアーのユーザ ロールを割り当て済みのロールから除外するには、[レポート ビューアー（Report Viewer）] オプションを手動で選択解除して [保存（Save）] をクリックします。

通常のシステム管理タスクの一部として、Cisco Prime Collaboration Assurance データベースからユーザを削除する必要がある場合があります。ただし、Cisco Prime Collaboration Assurance の Web クライアントのデフォルト管理者「globaladmin」は削除できません。

ユーザを削除するには、**[システム管理（System Administration）]** > **[ユーザ管理（User Management）]** でユーザを選択し、**[削除（Delete）]**をクリックします。削除したユーザ名でスケジュールされたジョブは、ジョブがキャンセルされるまで引き続き実行されます。

LDAP サーバの設定

Lightweight Directory Access Protocol（LDAP）サーバに保存されているユーザ情報にアクセスするために、Cisco Prime Collaboration Assurance を設定して LDAP サーバに接続することができます。

[ユーザ管理（User Management）] ページで LDAP ユーザを作成して、このユーザが LDAP のクレデンシャルを使用してログインできるようにする必要があります。ユーザを追加するには、「ユーザの追加」を、ユーザを編集または削除するには、「ユーザ ロールの変更」を参照してください。

Cisco Prime Collaboration Assurance は、1 つのプライマリ LDAP サーバと 1 つのバックアップ LDAP サーバをサポートしています。

LDAP サーバを設定するには、次の手順を実行します。

ステップ 1 選択 **[システム管理（System Administration）]** > **[LDAP設定（LDAP Settings）]**。

ステップ 2 [LDAP Settings] ページで、すべてのフィールドに値を入力します。フィールドの説明については、[LDAP Configuration] のパラメータを参照してください。

（注）

1. Cisco Prime Collaboration Assurance で SSL 暗号化を使用する必要がある場合は、[SSL を使用する（Use SSL）] チェックボックスをオンにして、ポート 636 を指定します。

   Cisco Prime Collaboration リリース 12.1 の場合

   SSL を有効にした LDAP 設定はサポートされていません。

2. 無効なログインの場合は、「ユーザ名またはパスワードが無効です。Please try again or check LDAP server configuration if you are a LDAP user（ユーザ名またはパスワードが無効です。もう一度やり直すか、LDAP ユーザの場合は LDAP サーバの設定を確認してください）」 というメッセージが表示されます。このメッセージは、ローカルと LDAP の両方のユーザに表示されます。

ステップ 3 LDAP サーバへの接続を確認するには、[テスト接続（Test Connection）] をクリックします。

ステップ 4 接続が正常に行われたら、[設定の適用（Apply Settings）] をクリックし、Cisco Prime Collaboration Assurance サーバを再起動して、LDAP を使用してログインします。

Cisco Prime Collaboration Assurance サーバを再起動するには、admin ユーザとしてログインし、次のコマンドを実行します。

```
application stop cpcm application start cpcm
```

application stop cpcm コマンドは実行完了までに 10 分、**application start cpcm** コマンドは実行完了までに 10 ～ 15 分かかります。

[LDAP Configuration] のパラメータ

たとえば、Microsoft Active Directory について考えてみましょう。

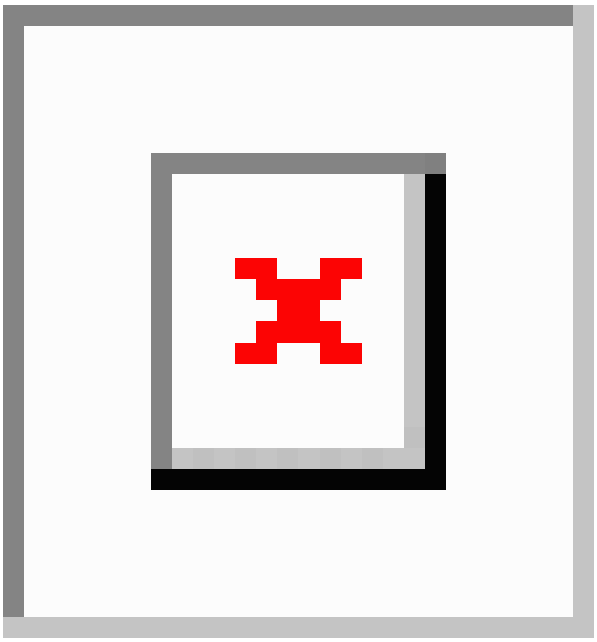


表 *10 : LDAP* サーバの設定

フィールド	説明
サーバの IP アドレス	LDAP サーバ名または IP アドレスを入力します。 オプションで、バックアップ LDAP サーバの IP アドレスを入力します。

フィールド	説明
サーバ ポート	サーバの LDAP 要求を受信するポート番号を入力します。 [Non-secure port]：389 [Secure SSL port]：636 オプションでバックアップLDAPサーバのポート番号を入力します。 （注） 標準以外のポートを使用するように LDAP サーバが設定されている場合は、そのポートもここで入力する必要があります。
Admin Distinguished Name	[Admin Distinguished Name] は使用する識別名です。 たとえば、前述のイメージでは、LDAP ディレクトリに John Doe という名前のユーザが 含まれていますが、[Admin Distinguished Name] は次のようになります。 • CN = John Doe • OU = Campus • OU = AdminBLR • OU = ABC • DC = eta • DC = com
管理者パスワード	LDAPサーバのパスワードを入力し、パスワードを再確認します。 （注） パスワードにシャープ記号（#）を使用しないでください。LDAP のユーザパスワードにシャープ記号が含まれていると、LDAP サーバへの接続が失敗します。

フィールド	説明
LDAP ユーザの検索ベース	ユーザの検索ベースを入力します。LDAPサーバはこのベースに基づいてユーザを検索します。 検索ベースは次のとおりです。 • DC = eta • DC = com （注） LDAP 認証は、検索ベースで特殊文字を入力すると失敗します。

（注）

1. Cisco Prime Collaboration Assurance は、必要に応じて、LDAP ユーザの CN、sAMAccountName、または uid 属性を使用した PCA へのログインをサポートします。
2. LDAP ユーザの uid 属性は一意である必要があります。
3. LDAPパラメータ値では、識別名（DN）でアンパサンド（&）を使用することはできません。

   LDAP に接続するには、次の LDAP パラメータ値を入力します。

   ```
   ?CN=hq-prime,OU=Service Access Groups,DC=Megafon,DC=ru?
   ```

サポートされている LDAP サーバの一覧については、「Cisco Prime Collaboration Assurance でサポートされているデバイス」を参照してください。

パスワードの最大数を設定

認証メカニズムは、そのクレデンシャルと同じだけの強度しかありません。

強力な認証メカニズムを使用することは、強力なパスワードを使用するために重要です。パスワードが複雑になっていない場合（特にパスワード長）、検索スペースが大幅に削減されます。

（注）

- デフォルトのパスワードの最大長は 127 文字です。
- デフォルトの管理者である globaladmin のみが、Cisco Prime Collaboration Assurance ユーザインターフェイスの [セキュリティ設定（security settings）] ページを変更する権限を持ちます。

ステップ 1 [システム管理（**System Administration**）] > [セキュリティ設定（**Security Settings**）] を選択します。

（注） ユーザは、80-127 文字（バイトではありません）の範囲で値を入力する必要があります。入力した値が範囲外の場合は、入力された値が許容範囲を超えていることを示すメッセージが表示されます。**[OK]** をクリックして続行します。

ステップ 2 値を入力するか、またはスピン ボックスをクリックして、パスワード長を設定します。

ステップ 3 [保存（Save）] をクリックして、設定の詳細を正常に更新します。アプリケーションは、ユーザがパスワードの最大長を変更していることをアラートします。「Ensure compliance with this new value while setting password in other pages」と表示されます。

[キャンセル（Cancel）] をクリックして終了します。

（注） ユーザは、他のページでパスワードが必要な場合に、ここで設定した値よりも長いパスワードを入力することはできません。コンプライアンスに従っていないことを示すエラー メッセージが、そのページに表示されます。

Cisco Prime Collaboration Assurance アカウントのロック解除

Cisco Prime Collaboration リリース 11.5 以降の場合

Cisco Prime Collaboration Assurance のユーザ インターフェイスへのログインの最大試行回数は 10 です。10 回試行しても、Cisco Prime Collaboration Assurance のユーザ インターフェイスにログインできない場合は、アカウントが無効になります。

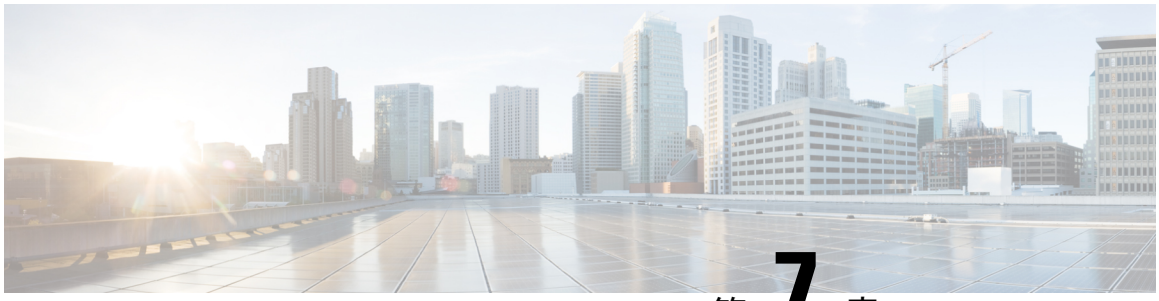
管理者権限を持つ globaladmin ユーザであれば、アカウントのロックを解除することができます。

アカウントのロックを解除するには、次のようにします。

ステップ 1 Cisco Prime Collaboration Assurance に globaladmin としてログインします。

ステップ 2 選択 **[システム管理（System Administration）]** > **[ユーザ管理（User Management）]**。

ステップ 3 **[ユーザ管理（User Management）]** ページで、ユーザを選択し、**[ロック解除（Unlock）]** をクリックします。



第 7 章

顧客の管理

このセクションでは、次の点について説明します。

- 顧客の管理 （87 ページ）
- 顧客の追加 （87 ページ）
- グローバル顧客の選択 （88 ページ）

顧客の管理

このセクションは、Cisco Prime Collaboration Assurance を MSP モードで導入した場合のみ適用されます。

MSP モードは複数のカスタマー ビューを提供します。このオプションは、マネージド サービス プロバイダーの環境で使用します。このビューでは、ネットワークを管理したり、Cisco Prime Collaboration Assurance によって管理されている複数の顧客のサービスをホストしたりすることができます。デバイスを顧客に関連付けることができます。

管理されている既存のすべてのエンドポイント、またはパブリッシャに登録されているサブスクライバが、パブリッシャからカスタマー名を継承するかどうかを選択できます。詳細については、「デバイスの追加 - 自動検出」を参照してください。

顧客の追加

顧客を追加するには、次の手順を実行します。

ステップ 1 を選択します。**[アシュアランス管理（Assurance Administration）]** > **[顧客管理（Customer Management）]**。

Cisco Prime Collaboration リリース 11.5 以降の場合

移行方法 **[アラームおよびレポート管理（Alarm & Report Administration）]** > **[顧客管理（Customer Management）]**

ステップ 2 [顧客管理 (Customer Management)] ページで、[追加（Add）] をクリックします。

ステップ 3 [一般情報（General Info）] ページで必要な詳細を入力し、[次へ（Next）] をクリックします。

ステップ 4 [デバイス/デバイスグループ（Devices/Device Group）] ページで適切なデバイスを選択し、[保存（Save）] をクリックします。選択したデバイスに対する顧客の割り当てを確認するように求めるメッセージが表示されます。ユニファイド CM または VCS などのパブリッシャまたはシードデバイスが関連付けられている顧客に、登録済みのエンドポイントを関連付けるには、**[登録済みのエンドポイントも割り当てる]** チェックボックスをオンにします。デバイスが顧客に関連付けられていることを通知するメッセージが表示されます。

関連トピック

ユーザの追加 （81 ページ）
[ユーザ管理（Manage Users）] （75 ページ）

グローバル顧客の選択

Cisco Prime Collaboration Assurance ホーム ページで、顧客を選択し、それに応じてフィルタリングできます。Cisco Prime Collaboration Assurance ユーザ インターフェイスの右上隅にある [顧客（Customer）] フィールドの横にある [クイックビュー（Quick View）] アイコンの上にマウスを合わせます。データを表示する 1 つ以上の顧客を選択できます。[すべての顧客（All Customers）] を選択して、すべての顧客の集約された情報を表示することにより、複数の顧客を同時に選択することもできます。デフォルトでは、すべての顧客のデータが表示されます。

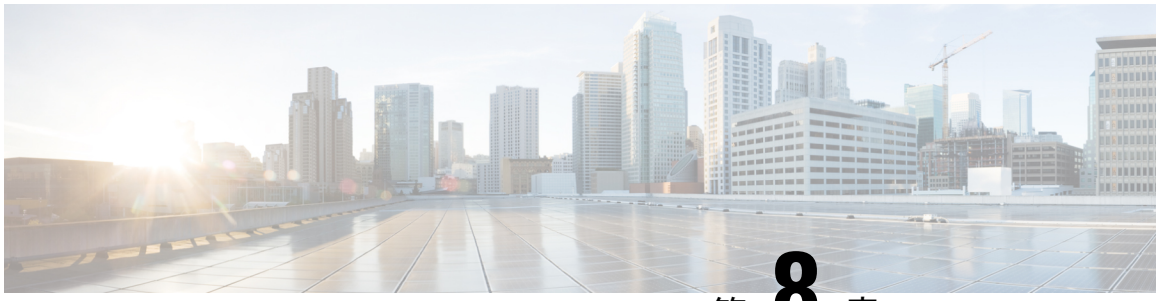
Cisco Prime Collaboration Assuranceで、特定の顧客に対応するユーザとして Cisco Prime Collaboration Assurance にログインしている場合は、グローバル顧客選択リストから [すべての顧客（すべての顧客）]オプションを選択できます。さらに、[すべての顧客（All My Customers）] グループから特定の顧客を選択できます。

Cisco Prime Collaboration Assurance で、すべての使用可能な顧客に対応するユーザ または globaladmin として Cisco Prime Collaboration Assurance にログインしている場合は、グローバル顧客選択リストから [すべての顧客（All Customers）] オプションを選択できます。さらに、[すべての顧客（All Customers）] グループから特定の顧客を選択できます。

Cisco Prime Collaboration Assurance のユーザ インターフェイスは、[][インベントリ管理（Inventory Management）]、[アラームおよびイベント（Alarms and Events）] ページなどのすべての機能全体で、グローバル選択フィールドからすべての顧客の情報をフィルタして表示します。

（注） Cisco Prime Collaboration Assurance エンタープライズ ダッシュボード（持っているライセンスに応じた End-Users Impact、Endpoints Utilization、Infrastructure、Topology、Contact Center トポロジ）は、デフォルトでは、グローバル顧客選択フィールドで内容をフィルタしません。グローバル選択によって別の顧客を選択すると、ユーザ インターフェイスが更新され、[カスタマーサマリ（Customer Summary）] ダッシュボードのホームページが表示されます。顧客を変更するには、[カスタマーサマリ（Customer Summary）] ダッシュボードで顧客名をクリックする必要があります。

ユーザ ロールが使用可能な情報を決定する方法の詳細については、「Cisco Prime Collaboration Assurance - 高度なユーザ ロール」を参照してください。



第 8 章

ドメインの管理

このセクションでは、次の点について説明します。

- ドメインの管理 （89 ページ）

ドメインの管理

このセクションでは、Cisco Prime Collaboration Assurance でのドメインの管理について説明します。

ドメインの管理

ドメイン管理機能は、エンタープライズ モードで Cisco Prime Collaboration Assurance をインストールした場合にサポートされます。ビジネス ニーズに応じてデバイスをグループ化し、一部のデバイス セットに制限付きのビューを提供することができます。

（注） Cisco Prime Collaboration Assurance は、ドメイン設定動作に応じて次のシナリオをサポートします。

1. 同じクラスタ内のすべてのエンドポイントを同じドメインに割り当てます。
2. Cisco Prime Collaboration Assurance では、同じクラスタ内の異なるエンドポイントに対して、異なるドメインを割り当てることはサポートしていません。
3. 異なるインフラストラクチャデバイスに対して、異なるドメインを割り当てることができます。

関連トピック

[ユーザ管理（Manage Users）] （75 ページ）

アシュアランスドメインの追加

Assurance をドメインに追加するには、次のようにします。

ステップ 1 選択 **[システム管理（System Administration）] > [ドメインのセットアップ（Domain Setup）]**。

ステップ 2 **[ドメインの設定（Domain Setup）]** ページで、**[追加（Add）]** をクリックします。デバイス プールまたはデバイスをドメインに関連付けることができます。

ステップ 3 [作成（Create）][Assurance（Assurance）][ドメイン（Domain）]ページで必要な詳細を入力し、[保存（Save）] をクリックします。

パブリッシャが単一のドメインに関連付けて検出された場合、パブリッシャに登録されたすべてのエンドポイントまたはサブスクライバは、パブリッシャから ドメイン名を継承します。

（注） 1 つのデバイスに複数のドメインを関連付けることはできません。

[編集（Edit）] をクリックして、 ドメインを割り当て解除します。

（注） デバイス プールのドメインを変更する場合は、新しいドメインに割り当てる前に、既存のドメインからデバイス プールを割り当て解除する必要があります。この制限は、デバイス プールのみ適用されます。

[削除（Delete）] をクリックしてドメインを削除します。ドメインの削除には、デバイスあり、またはデバイスなしを選択できます。[インベントリ管理（Inventory Management）] で変更を確認できます。

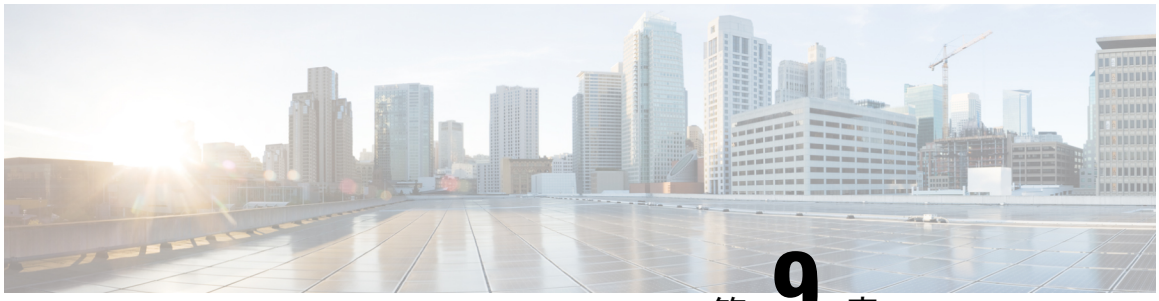
グローバルなドメインの選択

Cisco Prime Collaboration Assurance ホーム ページで、ドメインを選択し、それに応じてフィルタリングできます。Cisco Prime Collaboration Assurance ユーザ インターフェイスの右上隅にある [ドメイン（Domain）] フィールドの横にある [クイックビュー（Quick View）] アイコンの上にマウスを置きます。ドメイン権限に基づいて 1 つ以上のドメインを選択できます。

Cisco Prime Collaboration Assuranceで 利用可能なすべての ドメインに関連したユーザまたは globaladmin として Cisco Prime Collaboration Assurance にログインしている場合は、[エンタープライズ（Enterprise）] を選択すると、すべての ドメインの集約の詳細を表示できます。さらに、[マイ エンタープライズ（My Enterpris）] グループから特定の ドメインを選択できます。

Cisco Prime Collaboration Assurance ユーザ インターフェイスは、[インベントリ管理（Inventory Management）] および [エンドポイントの診断（Endpoint Diagnostics）] などの機能全体で、選択した ドメインの情報のみをフィルタして表示します。これらの列は、デフォルトでは非表示になっています。

ユーザ ロールが使用可能な情報を決定する方法の詳細については、「Cisco Prime Collaboration Assurance - 高度なユーザ ロール」を参照してください。



第 9 章

システム パラメータの設定

このセクションでは、次の点について説明します。

- システム パラメータの設定 （91 ページ）

システム パラメータの設定

Cisco Prime Collaboration Assurance のシステム設定パラメータは、次のとおりです。

- SMTP サーバ:このパラメータを次の下で設定します。 **[アシュアランス管理（Assurance Administration）] > [アラームとイベントの電子メール設定（E-mail Setup for Alarms & Events）]**SMTP サーバの設定を参照してください。

  Cisco Prime Collaboration リリース 11.5 以降の場合

  SMTPサーバ:このパラメータを次の下で設定します。**[アラームおよびレポート管理（Alarm & Report Administration）] > [アラームとイベントの電子メール設定（E-mail Setup for Alarms & Events）]**SMTP サーバの設定を参照してください。

- コール品質データソースの管理：Cisco Prime Collaboration Assurance は、VoIP ネットワークで音声品質の測定値を監視します。このリアルタイムによるサービス品質情報は、Unified CM、、またはPrime vNAMから収集されます。このパラメータを次の下で設定するには、次の手順に従います。 **[アシュアランス管理（Assurance Administration）] > [CDS ソース設定（CDR Source Settings）] > [通話品質データ ソース管理（Manage Call Quality Data Sources）]**CDR データ ソース コール詳細レコード NAM クレデンシャルの更新を参照してください。

  Cisco Prime Collaboration リリース 11.5 以降の場合

  コール品質データソースの管理：Cisco Prime Collaboration Assurance は、VoIP ネットワークで音声品質の測定値を監視します。このリアルタイムによるサービス品質情報は、Unified CM、、またはPrime vNAMから収集されます。このパラメータを次の下で設定するには、次の手順に従います。 **[アラームおよびレポート管理（Alarm & Report Administration）] > [CDS ソース設定（CDR Source Settings）] > [通話品質データ ソース管理（Manage Call Quality Data Sources）]**CDR データ ソース コール詳細レコード NAM クレデンシャルの更新を参照してください。

- [LDAP 設定（LDAP Settings）]：このパラメータを次の設定で設定します。**[システム管理（System Administration）] > [LDAP 設定（LDAP Settings）]**LDAP サーバの設定を参照してください。
- [ログの管理（Log Management）]：このパラメータを次の設定で設定します。**[システム管理（System Administration）] > [ログの管理（Log Management）]**ログ レベルを参照してください。
- SFTP 設定：Unified CM からのコールを監視するには、SFTP を設定する必要があります。このパラメータを次の下で設定するには、次の手順に従います。**[アシュアランス管理（Assurance Administration）] > [CDS ソース設定（CDR Source Settings）] > [CUCM SFTPクレデンシャル（CUCM SFTP Credentials）]**SFTP 設定項目の設定 を参照してください。

  Cisco Prime Collaboration リリース 11.5 以降の場合

  SFTP 設定：Unified CM からのコールを監視するには、SFTP を設定する必要があります。このパラメータを次の下で設定するには、次の手順に従います。**[アラームおよびレポート管理（Alarm & Report Administration）] > [CDR ソース設定（CDR Source Settings）] > [CUCM SFTP クレデンシャル（CUCM SFTP Credentials）]**SFTP 設定項目の設定 を参照してください。

  Cisco Prime Collaboration リリース 12.1 SP3 以降の場合

  SFTP 設定：Unified CM からのコールを監視するには、SFTP を設定する必要があります。このパラメータを次の下で設定するには、次の手順に従います。**[インベントリ（Inventory）] > [インベントリ管理（Inventory Management）]。[CUCM SFTP クレデンシャル（CUCM SFTP Credentials）]** タブをクリックし、SFTP 設定項目の設定 を参照してください。
- クラスタ デバイスの検出設定：Cisco Prime Collaboration Assurance が、Unified CM から収集したインベントリとデバイス登録情報を統合できるようにします。このパラメータを次の下で設定するには、次の手順に従います。**[インベントリ（Inventory）] > [クラスタ デバイス検出スケジュール（Cluster Device Discovery Schedule）]**クラスタ デバイスの検出をスケジュール （166 ページ）を参照してください。

グローバル システム パラメータ

これらのページで行った変更は、すべてのまたはドメイン（Enterprise モード）に適用されます。

表 *11* : システム パラメータ

タスク	ナビゲーション
シングル サインオンを設定します。	**[システム管理（System Administration）] > [シングル サインオン（Single Sign-On）]**

タスク	ナビゲーション
ライセンス ファイルを追加します。	**[システム管理（System Administration）]>[ライセンス管理（License Management）]**
SMTP サーバを設定します。	**[アラームおよびレポート管理（Alarm & Report Administration）]>[アラームとイベント用に電子メールをセットアップ（E-mail Setup for Alarms & Events）]**
デバイス検出のため SSL 証明書認証を設定します。	**[システム管理（System Administration）]>[証明書管理（Certificate Management）]**
ユーザの詳細にアクセスするため LDAP サーバを設定します。	**[システム管理（System Administration）]>[LDAP 設定（LDAP Settings）]**
ログレベルを変更します。デフォルト値は「[エラー（Error）]」 です。	**[システム管理（System Administration）]>[ログの管理（Log Management）]**
Unified CM からのコールを監視するため SFTP パラメータを設定します。	**[インベントリ（Inventory）]>[インベントリ管理（Inventory Management）]>[CUCM/sFTP クレデンシャル（CUCM/sFTP Credentials）]** **Cisco Prime Collaboration リリース 12.1 SP3 以降の場合** **[インベントリ（Inventory）]>[インベントリ管理（Inventory Management）]**。[CUCM SFTP クレデンシャル（CUCM SFTP Credentials）] タブをクリックします。
Unified CM でパラメータを設定して、インベントリとデバイスの登録情報を統合させます。	**[インベントリ（Inventory）]>[クラスタ デバイス検出スケジュール（Cluster Device Discovery Schedule）]**
ダイヤル プランを追加します。	**[アラームおよびレポート管理（Alarm & Report Administration）] > [CDR 分析の設定（CDR Analysis Settings）] > [ダイヤル プランの設定（Dial Plan Configuration）]**
コール カテゴリを作成します。	**[アラームとレポート管理（Alarm & Report Administration）]>[CDR 分析の設定（CDR Analysis Settings）]>[コール カテゴリの設定（Set Call Category）]**
パラメータを設定してデバイスをポーリングします。	**[アラームとレポート管理（Alarm & Report Administration）]>[ポーリング設定（Polling Settings）]**

タスク	ナビゲーション
Syslog ルールをカスタマイズして不具合を監視します。	**[アラームおよびレポート管理（Alarm & Report Administration）] > [イベントのカスタマイズ（Event Customization）] > [Syslog ルール（Syslog Rules）]**
アラーム通知（電子メール、syslog、トラップ）を設定します。	**[アラームおよびレポート管理（Alarm & Report Administration）] > [通知のセットアップ（Notification Setup）] > [カスタム通知（Custom Notification）]**
音声コールグレード設定（Good、Acceptable、Poor）を構成します。	**[アラームとレポート管理（Alarm & Report Administration）] > [CDR 分析の設定（CDR Analysis Settings）] > [音声コールグレードの設定（Configure Voice Call Grade）]**
音声電話レポート（IP フォンの監査、移動、疑いのある IP フォン）、ファイル形式、エクスポート ファイルの場所、電子メール通知など、音声電話レポートのエクスポートパラメータを設定します。	**[レポート（Reports）] > [UCM/CME Phone Activity Reports] > [音声電話のエクスポート（Export Audio Phones）]**
定期的なバックアップをスケジュール設定します。	**[システム管理（System Administration）] > [バックアップ設定（Backup Settings）]**

SMTP サーバの設定

SMTP サーバ名と送信者 AAA 電子メール アドレスを、**[アラームとイベントの電子メール設定（E-mail Setup for Alarms & Events）]** ページ（**[アラームとイベントの電子メール設定（E-mail Setup for Alarms & Events）]**）で指定することで、アラームの電子メール通知を送受信するように SMTP サーバを設定することができます。[Sender AAA E-mail Address] フィールドの値は、多数のサーバがある場合に、電子メールを受信したサーバを特定するのに便利です。

Cisco Prime Collaboration Assurance サーバのタイム ゾーンの設定

Cisco Prime Collaboration Assurance サーバのタイム ゾーンを設定するには、次の手順を実行します。

ステップ 1 インストールで作成したアカウントを使用して Cisco Prime Collaboration Assurance サーバにログインします。デフォルト設定は、*admin* です。

ステップ 2 次のコマンドを入力して、サポートされているタイム ゾーンのリストを表示します。

例：

```
cm/admin# show timezones
```

ステップ 3 Cisco Prime Collaboration Assurance サーバのタイム ゾーンを設定するには、次のコマンドを入力します。

例：

```
cm/admin(config)# config t cm/admin(config)# clock timezone US/Pacific cm/admin(config)# exit
```

ステップ 4 実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーするには、次のコマンドを入力します。

例：

```
cm/admin# write memory
```

ステップ 5 Cisco Prime Collaboration Assurance サーバを再起動するには、次のコマンドを入力します。

例：

```
cm/admin# application stop cpcm cm/admin# show application status cpcm cm/admin# application start
 cpcm
```

ステップ 6 再起動プロセスが終了するまで 10 分間待機してから次のコマンドを入力し、タイム ゾーンが新しい値に設定されているかどうかを確認します。

例：

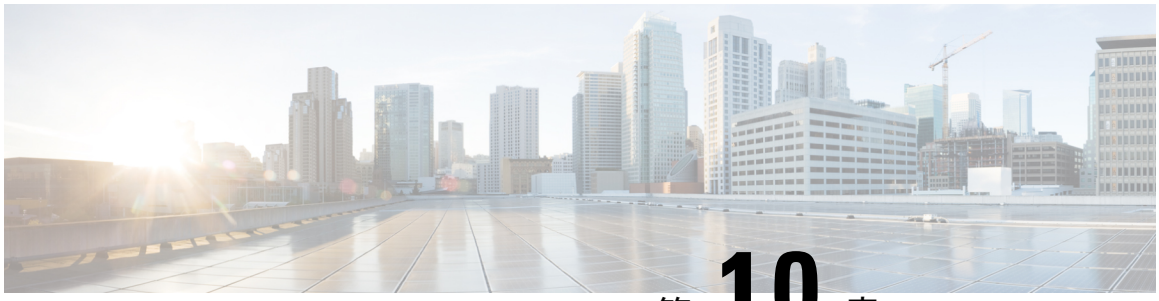
```
cm/admin# show timezone US/Pacific
```

（注） データの不一致を回避するために、postgres データベースで設定したタイム ゾーンの値をシステムのタイム ゾーンの値と同じにすることをお勧めします。システムのタイム ゾーンを手動で変更する場合は、cpcm データベースと qovr データベースの両方を含めて、`/opt/postgres/9.2/data`（Analytics データベース）および `/opt/postgres/9.2/cpcmdata`（Assurance データベース）の `postgres.conf` ファイルで log_timezone パラメータおよび timezone パラメータをシステムのタイム ゾーンと一致するように変更して、システムを再起動します。postgres データベースでタイム ゾーンの値を変更する場合は、root アクセス機能が必要です。そのため、root アクセス権を取得するために TAC ケースを送信する必要があります。

第 III 部

Cisco Prime Collaboration Assurance でのデバイスの管理

- デバイス クレデンシャルの管理 （99 ページ）
- クラスタのセットアップ （125 ページ）
- デバイスの検出 （129 ページ）
- デバイス グループの管理 （173 ページ）
- インベントリの管理 （179 ページ）
- ポーリング デバイス （237 ページ）



第 10 章

デバイス クレデンシャルの管理

このセクションでは、次の点について説明します。

- デバイス クレデンシャルの管理 （99 ページ）
- デバイス クレデンシャル プロファイルの追加 （100 ページ）
- デバイス ディスカバリの SSL 証明書認証 （118 ページ）
- デバイス クレデンシャルの変更 （118 ページ）
- デバイス クレデンシャルの確認 （119 ページ）
- デバイス クレデンシャル プロファイルの削除 （123 ページ）

デバイス クレデンシャルの管理

Cisco Prime Collaboration Assurance を使用して管理するすべてのデバイスのデバイス クレデンシャルを設定する必要があります。デバイスを検出し、インベントリを更新するためにデバイス クレデンシャルが必要です。クレデンシャルがデバイスによって異なる場合は、別のクレデンシャル プロファイルを作成します。つまり、Cisco Prime Collaboration Assurance の 2 つの Cisco Unified Communications Manager を異なるクレデンシャルで管理する場合、2 つのクレデンシャル プロファイルを作成する必要があります。詳細については、[Credential Profiles] のフィールドの説明表を参照してください。

次は、クレデンシャル プロファイルを作成する際のいくつかの要件です。

- エンドポイントが Managed 状態になるまで、HTTP と SNMP にはクレデンシャルが必要です。
- **Cisco Prime Collaboration リリース 11.1 以前の場合**

  エンドポイントとネットワーク デバイスに関連するセッションをトラブルシュートするには、CLI クレデンシャルが必要です。
- **Cisco Prime Collaboration リリース 11.5 以降の場合**

  CLI クレデンシャルは、ビデオ テスト コールを管理し、SIP Call Flow Analyzer を介したコール シグナリングの分析に必要です。

- Unified CM の会議監視には、JTAPI クレデンシャルが必要です。このクレデンシャルは、エンドポイントでは必要ありません。
- Enterprise License Manager プロファイルを作成するには、Prime License Manager のデバイス タイプで Enterprise License Manager を選択します。
- Cisco Unified Intelligence Center（CUIC）、Cisco Voice Portal（CVP）、Cisco Finesse、Cisco SocialMiner、Cisco Unified Contact Center Enterprise（Unified CCE）、Cisco Unified Contact Center Express（Unified CCX）、Cisco MediaSense などの Unified Contact Center デバイスで、HTTP および SNMP のクレデンシャルを定義します。

  Cisco Prime Collaboration リリース 11.5 以降の場合

  Cisco Unified Intelligence Center（CUIC）、Cisco Voice Portal（CVP）、Cisco Finesse、Cisco SocialMiner、Cisco Unified Contact Center Enterprise（Unified CCE）、Cisco Unified Contact Center Express（Unified CCX）、Cisco Virtualized Voice Browser などの Unified Contact Center デバイスで、HTTP および SNMP のクレデンシャルを定義します。
- Contact Center Enterprise の HTTP クレデンシャルを domain\administrator のフォーマットで入力します。たとえば、hcsdc2\administrator となります。
- *ServiceabilityAdministrationUserRole* 権限を持つ Cisco Unified Customer Voice Portal（CVP）の HTTP クレデンシャルを入力します。この権限は、デフォルトのユーザ名である *wsmadmin* に与えられています。
- クレデンシャルは、電話機、Cisco Cius、Cisco Jabber、TelePresence（Movi）エンドポイント用の Cisco Jabber Video には必要ありません。これらのエンドポイントは、登録されているコール プロセッサの検出を介して検出されます。
- [デバイス（Device）] タイプのドロップダウン リストから [VCS/EXPRESSWAY] を選択し、Cisco Expressway-Core、Cisco Expressway-Edge、Cisco Collaboration Edge または Core を備えた Cisco VCS のクレデンシャルを作成します。

（注）
- [クレデンシャル プロファイル（Credential Profile）] ページでクレデンシャル プロファイルを作成、または [デバイス検出（Device Discovery）] でデバイスを追加するときに、SNMP Community String、SNMPv3、HTTP、JTAPI、MSI の 8 文字のパスワードで * 記号を使用することはできません。
- [クレデンシャル プロファイル（Credential Profile）] ページでクレデンシャル プロファイルを作成、または [デバイス検出（Device Discovery）] でデバイスを追加するときに、CLI の 8 文字のパスワードで % 記号を使用することはできません。

デバイス クレデンシャル プロファイルの追加

クレデンシャル プロファイルを追加または複製するには、次の手順を実行します。

ステップ 1 **[Cisco Prime Collaboration Assurance]** ページ で、 **[デバイスインベントリ（Device Inventory）]** > **[インベントリ管理（Inventory Management）]** [ナビゲーションの切り替え（Toggle Navigation）] ペインから上記の順に選択します。

Cisco Prime Collaboration リリース 11.5 以降の場合

[Cisco Prime Collaboration Assurance] ページ で、 **[インベントリ（Inventory）]** > **[インベントリ管理（Inventory Management）]** [ナビゲーションの切り替え（Toggle Navigation）] ペインから上記の順に選択します。

[Inventory Management] ページが表示されます。

ステップ 2 [クレデンシャルプロファイル（Credentials Profile）] ページで [追加（Add）] をクリックし、[Credential Profiles] のフィールドの説明 （101 ページ）の表で説明している必要な情報を入力します。

ステップ 3 **[保存（Save）]** をクリックします。

ネットワーク内で、すべてのデバイスに同じ SNMP クレデンシャルを設定している場合があります。このような場合は、まずプロファイルを新規に作成した後で、既存のプロファイルを複製してください。複製するには、[Credentials Profile] ページで既存のプロファイルを選択して [Clone] をクリックし、必要な更新をした後で [Add/Update] をクリックします。

[Credential Profiles] のフィールドの説明

デバイスの検出後、現在のインベントリ テーブルを確認し、Cisco Prime Collaboration Assurance データベースでクレデンシャルが更新されているかどうか確認できます。

次の表で [Credential Profiles] ページのフィールドについて説明します。

表 *12 : [Credential Profiles]* のフィールドの説明

フィールド名	説明
プロファイル名	クレデンシャル プロファイルの名前です。 次に例を示します。 • CUCM • router_switches

フィールド名	説明
デバイスタイプ	（任意）選択したデバイス タイプに基づき、クレデンシャル フィールド（SNMP、HTTP、CLI など）が表示されます。 再検出時間を短縮するため、クレデンシャル プロファイルを作成するときにデバイス タイプを選択することを推奨します。 クレデンシャル プロファイルを作成する際にデバイス タイプを選択しない場合、デフォルトのデバイス タイプは [任意（Any）] 「」になります。 デバイスタイプのリストについては、cisco.com を参照してください。 EX シリーズ、MXシリーズ、SXシリーズ、ベア コーデック デバイス、およびコーデックが指定されたすべてのプロファイルについては、デバイス タイプとして [TC_CE] を選択します。 共存型の PLM を管理している間は、CLI および HTTP クレデンシャルの両方を提供する必要があります。 • CLI クレデンシャルは、ライセンス情報にアクセスするために使用します。 • HTTP クレデンシャルは、Cisco Prime Collaboration Assurance で Prime License Manager を管理するために使用します。

フィールド名	説明
デバイス タイプ	

フィールド名	説明
	Cisco Prime Collaboration リリース 12.1 以降の場合 共存型の PLM を管理している間は、CLI および HTTP クレデンシャルの両方を提供する必要があります。 • CLI クレデンシャルは、ライセンス情報にアクセスするために使用します。 • HTTP クレデンシャルは、Cisco Prime Collaboration Assurance で Prime License Manager を管理するために使用します。 ルータが Cisco Unified Border Element（CUBE）として識別されるには、次の条件を満たす必要があります。 1. デバイス タイプ（ルータ）の CLI クレデンシャル情報（CLI ログイン ユーザ名および CLI ログイン パスワード）は必須です。 2. ルータの ポート 22 では SSH バージョン 2 以降を有効にする必要があります。 3. ルータで [パスワードの有効化（Enable Password）]が設定されている場合は、[CLI パスワード有効化（CLI Enable Password）] フィールドにパスワードを入力します。 **Cisco Prime Collaboration リリース 11.6 以降の場合** CE イメージ搭載の EX シリーズ、MX シリーズ、SX シリーズ、DX シリーズ、ベアなコーデック デバイス、コーデック付きのすべてのプロファイルでは、デバイス タイプとして [コーデック（コーデック）] を選択します。 MSEデバイスの場合は、デバイスタイプとして [Cisco MCU] を選択します。 **Cisco Prime Collaboration リリース 11.5 以降の場合** Virtualized Voice Browser デバイスの場合は、[Virtualized Voice Browser] デバイス タイプを選択します。

フィールド名	説明
	任意のクレデンシャル（SNMP、HTTP、CLI、MSI）を入力して、「[任意（Any）]」のクレデンシャル プロファイルを作成できます。自動検出（Ping スイープと CDP 検出）を実行するには、[任意（Any）]「」のクレデンシャル プロファイルを作成する必要があります。ただし、論理検出も実行できます。 ネットワークに複数のサブネットがある場合は、サブネットごとに [任意（Any）]「」のプロファイルを作成します。
IP バージョン	IP アドレスはバージョン 4 またはバージョン 6 です。

フィールド名	説明
IP アドレス パターン	

フィールド名	説明
	クレデンシャルを指定するデバイスの IP アドレスです。次の作業が必要です。 • 複数の IP アドレスはパイプ文字（|）で区切ります。 • 0.0.0.0 および 255.255.255.255 は使用しないでください。 • 疑問符（?）は使用しないでください。 次のことを行うことを推奨します。 • Cisco Unified CM、Cisco TMS に IP アドレスを正確に入力します。 • CTS またはネットワーク デバイスのいずれかの IP アドレスを正確に入力します。 • アドレス パターンではワイルドカード式を多数使用しないでください。 次に例を示します。 • 100.5.10.*|100.5.11.*|100.5.20.*|100.5.21.* • 200.5.1*.*|200.5.2*.*|200.5.3*.* • 172.23.223.14 • 150.5.*.* 150.*.*.* や 192.78.22.1? などのパターンの使用は避けます。150.5.*.*/24. デバイスの共通パターンが見つからない場合は、*.*.*.* と入力します。 クレデンシャルプロファイルで IP アドレスのパターンを定義するときには、できるだけワイルドカード文字（*）の使用を避けます。 **Cisco Prime Collaboration リリース 11.5 以降の場合** **[インベントリ（Inventory）] > [インベントリ管理（Inventory management）] > [クレデンシャルの管理（Manage Credentials）]** ワイルドカード文字を使用すると、検出時間が長くなる可能性があります。 パターンの使用方法については、SNMPv2C を

フィールド名	説明
	参照してください。
一般的な SNMP オプション	[SNMP Timeout]：デフォルトは 10 秒です。
	[SNMP Retries]：デフォルトは 2 です。
	[SNMP Version]：SNMP バージョンを選択する必要があります。
SNMPv2C デバイスの検出と管理に使用されます。	SNMP Read Community String SNMPv2C または SNMPv3 のいずれかのクレデンシャルを指定できます。Cisco TelePresence システムとネットワーク デバイスには異なる SNMP クレデンシャルを使用することを推奨します。 Cisco Prime Collaboration Assurance は、IP アドレスのパターンに基づきクレデンシャル プロファイルを検索します。次に、Cisco Prime Collaboration Assurance は SNMP クレデンシャルに一致するプロファイルを選択します。一致する複数のプロファイル（つまり、同じ SNMP クレデンシャルを持つプロファイル）が存在することがあります。この場合、Cisco Prime Collaboration Assurance は最初に一致するプロファイルを選択します。 **Cisco Prime Collaboration リリース 11.1 以前の場合** （注） 複数のプロファイルで同じ SNMP クレデンシャルを使用し、CLI クレデンシャルが異なる場合、Cisco Prime Collaboration Assurance はデバイスで正しい SNMP クレデンシャルを選択しますが、間違った CLI クレデンシャルを選択する場合があります。この場合、トラブルシューティング ワークフローが機能しないことがあります。
	SNMP Write Community String

フィールド名	説明
SNMPv3 デバイスの検出と管理に使用されます。	[SNMP Security Name]：セキュリティ名を入力します。
	[SNMP Authentication Protocol]：MD5 または SHA を選択できます。
	[SNMP Authentication Passphrase]：パスフレーズを入力します。
	SNMP Privacy Protocol：AES、AES128、または DESMD5 を選択できます。 **Cisco Prime Collaboration リリース 11.5 以降の場合** SNMP Privacy Protocol：AES128 または DES を選択できます。

フィールド名	説明
CLI トラブルシューティングの目的でメディア パスを検出するために、CLI を介してデバイスにアクセスするために使用されます。	[CLI Login Username] と [Password] CLI クレデンシャルは、トラブルシューティング ワークフロー中に使用されます。クレデンシャルが入力されていない場合、または入力されたクレデンシャルが正しくない場合、トラブルシューティング ワークフローは機能しないことがあります。 **Cisco Prime Collaboration リリース 11.5 以降の場合** CLI クレデンシャルは、ビデオ テスト コールを管理し、SIP Call Flow Analyzer を介したコール シグナリングの分析に使用します。 **Cisco Prime Collaboration リリース 12.1 以降の場合** ルータが Cisco Unified Border Element（CUBE）として識別されるには、次の条件を満たす必要があります。 **1.** デバイス タイプ（ルータ）の CLI クレデンシャル情報（CLI ログイン ユーザ名および CLI ログイン パスワード）は必須です。 **2.** ルータの ポート 22 では SSH バージョン 2 以降を有効にする必要があります。 **3.** ルータで [パスワードの有効化（Enable Password）]が設定されている場合は、[CLI パスワード有効化（CLI Enable Password）] フィールドにパスワードを入力します。
HTTP システム ステータスと会議情報をポーリングするために HTTP を介してデバイスにアクセスするために使用されます。	[HTTP Username] と [Password] Cisco Prime Collaboration Assurance は、最初にHTTP用のアクセスを確認します。アクセス試行に失敗した場合、Cisco Prime Collaboration Assurance は HTTPS 用のアクセスをチェックします。 <domain/username> の形式で Cisco TMS にログインした場合、[HTTPS Username] フィールドに同じ<domain/username> 値を追加してください。

フィールド名	説明
JTAPI Cisco Unified CM からセッション ステータス情報を取得する際に使用します。	（オプション）JTAPIユーザ名とパスワード。 （注） パスワードにはセミコロン（;）または等号（=）を使用しないでください。

フィールド名	説明

フィールド名	説明
	Cisco Prime Collaboration リリース 11.5 以降の場合 Cisco Unified CM からセッション ステータス情報を取得する際に使用します。 **Cisco Prime Collaboration リリース 12.1 SP1 の場合** 安全な JTAPI（TLS v1.2）接続を確立するため、JTAPI 固有の新しいパラメータ セットが導入されました。 （注） 1. CTI、JTAPI、および TAPI アプリケーションを保護する方法の詳細や、Certificate Authority Proxy Function の詳細については、『Cisco Unified Communications Manager のセキュリティ ガイド』の「CTI、JTAPI、TAPI の認証と暗号化のセットアップ」および「Certificate Authority Proxy Function」の各章を参照してください。 2. CUCM が [Mixed} モードであることを確認します。 JTAPI 固有のパラメータ セットは、次のとおりです。 1. **[セキュア接続（Secure Connection）]** チェックボックス 1. **チェックボックスをオンにする**：このオプションをオンにすると、Cisco Unified Communications Manager へのセキュアな TLS 接続が有効になります。 「この JTAPI ユーザには、その他の必要なロールとともに、[Standard CTI Secure Connection] ロールが関連付けられていることを確認します」という警告メッセージが表示されます。[OK] をクリックして、Cisco Prime Collaboration Assurance に戻ります。

フィールド名	説明
	2. **チェックボックスをオフにする**：このチェックボックスをオフにすると、JTAPI はセキュアな接続を確立できません。 「この JTAPI ユーザに関連付けられた [Standard CTI Secure Connection] ロールが削除されていることを確認します」という警告メッセージが表示されます。[Monitor Conferences] へと続行するには、必要な役割が設定されていることを確認します。[OK] をクリックして、Cisco Prime Collaboration Assurance に戻ります。 詳細については、「Cisco Prime Collaboration Assurance 用のデバイスをセットアップ」を参照してください。 チェックボックスを使用すると、新しい Secure JTAPI フィールドにパラメータを入力できます（有効または無効）。

フィールド名	説明

フィールド名	説明
	２．**TFTP サーバ IP アドレス**：TFTP サーバの IP アドレスを指定します。 （注） この値は、CUCM クラスタのいずれかのノードである必要があります。そのノードで、TFTP サービスが実行されていることを確認します。 **3. TFTP サーバ ポート**：TFTP サーバ ポートのデフォルト値は 69 です。 （注） システム管理者に推奨されない限り、デフォルト値は変更しないようにします。 **4. CAPF サーバ IP アドレス**：CAPF サーバの IP アドレスを指定します。 （注） **1.** 証明書の認証プロキシ機能の詳細については、『Cisco Unified Communications Manager 用のセキュリティ ガイド』の「証明書の認証プロキシ機能」の章を参照してください。 **2.** CUCM で CAPF プロファイルを作成するときは、**[キーの順序（Key Order）]** ドロップダウンリストから **[RSA のみ（RSA Only）]** を選択してください。 **3.** CUCM Publisher IP アドレスは、常に指定する必要があります。 **5. CAPF サーバ ポート**：CAPF サーバ ポート番号のデフォルト値は 3804 です。 （注） 入力した値が、Cisco Unified Communication Manager で設定された値と一致していることを確認します。 **7. パブリッシャ用のインスタンス ID**：このフィールドには、アプリケーションの CAPF 設定、または Cisco Unified Communication Manager クラスタのエンド ユーザ CAPF のプ

フィールド名	説明
	ロファイル設定ページで設定した、アプリケーション インスタンスの識別子を指定します。 **8. セキュア認証文字列**：アプリケーションの CAPF 設定セクション、または各 Communication Manager Publisher のエンドユーザ CAPF のプロファイル設定ページで設定した認証文字列を入力します。 （注） セキュアな JTAPI 接続のトラブルシューティングセクションには、考えられるエラーに対するトラブルシューティングの詳細や、Conference Diagnostics が捉えることのできない CUCM for Secure JTAPI and Sessions のセットアップで推奨されるアクションが一覧表示されます。

Cisco Prime Collaboration リリース 11.5 以降の場合

[クレデンシャル プロファイル（Credential Profiles）] ページでは、次のデバイスの名前が変更されています。

- CISCO INTERACTION MANAGER から WEB/EMAIL INTERACTION MANAGER に名前変更
- CUIC から INTELLIGENCE CENTER に名前変更
- CTS から CTS/IX ENDPOINT に名前変更
- CISCO UNIFIED COMMUNICATIONS MANAGER から COMMUNICATIONS MANAGER に名前変更
- C_SERIES CODEC から TC/CE ENDPOINT に名前変更
- E20 から E20 ENDPOINT に名前変更
- ISDN から ISDN GATEWAY に名前変更
- MCU から MULTIPOINT CONTROLLER に名前変更
- MXP から MXP ENDPOINT に名前変更
- ROUTER から ROUTER/VOICEGATEWAY に名前変更
- TPS から TELEPRESENCE SERVER に名前変更
- TELEPRESENCE CONDUCTOR から TELEPRESENCE CONDUCTOR に名前変更

（注） Cisco デバイス、、Cisco Unified Communications Manager Express（Cisco Unified CME）、UC500 シリーズ デバイスでは、[クレデンシャル プロファイル（Credential Profiles）] ページにクレデンシャルを追加する必要はありません。

デバイス ディスカバリの SSL 証明書認証

Cisco Prime Collaboration リリース 11.1 以前の場合

Cisco Prime Collaboration Assurance では、デバイスが追加されると、HTTPS を使用して保護されたリソースにアクセスすることによって、クレデンシャル検証用の SSL 証明書が交換されます。SSL 証明書は交換中に Cisco Prime Collaboration Assurance の信頼ストアに保存されないため、その後のそのデバイスとの通信は失敗します。このデバイスにアクセスするには、SSL 証明書を手動で Cisco Prime Collaboration Assurance の信頼ストアにインポートすることをお勧めします。

Cisco Prime Collaboration Assurance では、HTTPS でのデバイスまたはアプリケーションとの通信中に SSL 証明書の信頼性を確認することができます。ただし、この場合でも証明書を認証せずにデバイスの検出を続行するため、これは必須ではありません。

デフォルトでは、Cisco Prime Collaboration Assurance は通信するデバイスまたはアプリケーションからの証明書を検証しません。

SSL 証明書認証を有効にするには:

ステップ 1 選択 **[システム管理（System Administration）]** > **[証明書管理（Certificate Management）]**。
[証明書の管理（Certificate Management）] ページが表示されます。

ステップ 2 [デバイス証明書の管理（Device Certificate Management）] タブで、[デバイス検出のための SSL 証明書認証を有効にする（Enable SSL certificate authentication for device discovery）] チェックボックスをオンにします。

ステップ 3 [Import Certificates] ボタンをクリックします。

ステップ 4 Cisco Prime Collaboration Assurance を再起動し、信頼マネージャ内の変更を有効にします。

```
cm/admin# application stop cpcm
cm/admin# show application status cpcm
cm/admin# application start cpcm
```

デバイス クレデンシャルの変更

Cisco Prime Collaboration Assurance アプリケーションで現在管理しているデバイス クレデンシャルを変更した場合は、Cisco Prime Collaboration Assurance データベースで、関連するクレデンシャル プロファイルを変更する必要があります。

ログイン情報に誤りがある場合、デバイスにアクセスできないという重大イベントが Cisco Prime Collaboration Assurance からトリガーされます**[モニタ（Monitor）] > [アラームおよびイベント（Alarms & Events）] > [イベント（Events）]**。

クレデンシャル プロファイルを編集するには：

ステップ 1 選択 **[デバイスインベントリ（Device Inventory）] > [インベントリ管理（Inventory Management）]**。

Cisco Prime Collaboration リリース 11.5 以降の場合

移行方法 **[インベントリ（Inventory）] > [インベントリ管理（Inventory Management）]**

ステップ 2 [インベントリ管理（Inventory Management）] ページでデバイスを選択し、**[クレデンシャルの変更（Modify Credentials）]**をクリックし ます。

ステップ 3 [Credential Profiles] のフィールドの説明 （101 ページ） の表の説明に従って、クレデンシャルを更新します。

ステップ 4 **[再検出（Rediscover）]** をクリックします。

Cisco Prime Collaboration Assurance では、変更したクレデンシャルでデータベースが更新されるのに数分かかります。クレデンシャルの更新後に、情報イベントの Device is accessible from Collaboration Manager がトリガーされます。Cisco Prime Collaboration Assurance では、次のポーリング ジョブで更新されたクレデンシャルが使用されます。

デバイス クレデンシャルの確認

Cisco Prime Collaboration リリース 11.5 以降の場合

クレデンシャルの誤りが原因でデバイス検出が失敗した場合は、失敗したデバイスのクレデンシャルをテストしてそのデバイスを再検出できます。選択 **[Device Inventory（デバイスインベントリ）] > [インベントリ管理（Inventory Management）] > [検出ジョブ（Auto Jobs）]** を選択すると、検出されなかったデバイスが一覧表示されます。

（注） 検出ジョブの実行中にこの作業を実行しないでください。

デバイス クレデンシャルを確認するには、以下を実施します。

ステップ 1 **Cisco Prime Collaboration リリース 11.5 以降の場合**

移行方法 **[インベントリ（Inventory）] > [インベントリ管理（Inventory Management）]**。

[Inventory Management] ページが表示されます。

ステップ 2 [Credential Profiles] ページから、クレデンシャルのテストに使用するプロファイル名を選択し、[Verify] をクリックします。

ステップ 3 クレデンシャルをテストするために有効なデバイスの IP アドレスを入力します。検証できるのは一度に 1 つのデバイスだけです。*.*.*.* や 192.2.*.* などの式は入力できません。

ステップ 4 [Test] をクリックします。タスクが完了するまで、テスト ボタンの横に処理中アイコンが表示されます。テスト結果は、[Test Credential Result] ペインの下に表示されます。

検証に失敗した場合は、「クレデンシャル検証のエラー メッセージ」に記載される、可能性のある理由を確認してください。

（注） クラスタ内のすべてのノードがすべてのプロトコルを実行するとは限りません。たとえば、JTAPI がすべてのノードでは実行されないこともあります。その結果、クレデンシャル検証テストが一部のノードで不合格となることがあります。クレデンシャルの問題点を解消したら、デバイス クレデンシャルを再度検証し、そのデバイスの検出を実行します。デバイスが検出されたら、[現在のインベントリ（Current Inventory）] テーブル内の Cisco Prime Collaboration Assurance データベースでアクセス情報が更新されたかどうかを確認できます。

クレデンシャル検証のエラー メッセージ

クレデンシャル検証のエラー メッセージを次の表に示します。

表 *13 :* クレデンシャル検証のエラー メッセージ

エラー メッセージ	条件	解決策
SNMPv2		
SNMP Request: Received no response from *IP Address*.	次のいずれかの原因により失敗。 • デバイスの応答が遅い。 • デバイスが到達不能である。 • クレデンシャル プロファイルに入力されたコミュニティ ストリングが正しくない	• デバイスの接続性を検証する。 • 正しいコミュニティ ストリングを指定してクレデンシャル プロファイルを更新する
SNMP timeout.	デバイスの応答が遅いか、またはデバイスが到達不能である。	• デバイスの接続性を検証する。 • クレデンシャル プロファイルで [SNMP Timeout] および [SNMP Retries] の値を大きくする。

エラー メッセージ	条件	解決策
Failed to fetch table due to: Request timed out.	デバイスの応答が遅いか、またはデバイスが到達不能である。	クレデンシャル プロファイルで [SNMP Timeout] および [SNMP Retries] の値を大きくする。
SNMPv3		
The configured SNMPv3 security level is not supported on the device.	設定された SNMPv3 セキュリティ レベルがデバイスでサポートされていない。	クレデンシャル プロファイルで、SNMPv3 セキュリティ レベルを、サポートされているセキュリティ レベルに変更する。
The SNMPv3 response was not received within the stipulated time.	デバイスの応答が遅いか、またはデバイスが到達不能である。	デバイスの接続性を検証する。
SNMPv3 Engine ID is wrong.	クレデンシャル プロファイルに入力されたエンジン ID が正しくない。	クレデンシャル プロファイルで、正しい SNMPv3 エンジン ID を入力する。
SNMPv3 message digest is wrong.	次のいずれかの原因により失敗。 • SNMPv3 認証アルゴリズムまたはデバイス パスワードが正しくない • ネットワーク エラー	• クレデンシャル プロファイルに正しい SNMPv3 認証アルゴリズムおよびデバイス パスワードが設定されていることを確認する • ネットワーク エラーがないかどうかを確認する
SNMPv3 message decryption error.	SNMPv3 メッセージを復号化できない。	クレデンシャル プロファイルに正しい SNMPv3 認証アルゴリズムが入力されていることを確認する。
Unknown SNMPv3 Context.	クレデンシャル プロファイルに設定されている SNMPv3 コンテキストがデバイスに存在しない。	クレデンシャル プロファイルに設定されている SNMPv3 コンテキストが正しいことを確認する。
Unknown SNMPv3 security name.	クレデンシャル プロファイルに設定された SNMPv3 ユーザ名が正しくない、またはデバイスで SNMPv3 ユーザ名が設定されていない。	クレデンシャル プロファイルおよびデバイスで正しい SNMPv3 ユーザ名が設定されていることを確認する。

エラー メッセージ	条件	解決策
CLI		
Login authentication failed.	クレデンシャル プロファイルに入力されたクレデンシャルが正しくない。	クレデンシャル プロファイルで、デバイスの CLI クレデンシャルを確認し再入力する。
Connection refused.	デバイス上で SSH サービスまたは Telnet サービスが実行されていない可能性がある。	1. サポートされている CLI（ポート）についてデバイスの接続性を検証する。 2. デバイス上で SSH サービスまたは Telnet サービスが実行されているかどうかを確認する
HTTP		
Server returned HTTP response code: 401 for URL.	HTTP サービスが実行されていない、または URL が無効である。	• デバイス上で HTTP サービスまたは HTTPS サービスが実行されているかどうかを確認する • サーバで URL が有効かどうかを確認する
Connection refused.	HTTP サービスまたは HTTPS サービスが実行されていない。	デバイス上で HTTP サービスまたは HTTPS サービスが実行されているかどうかを確認する
HTTP check failed.	クレデンシャル プロファイルに入力された HTTP クレデンシャルが正しくない。	クレデンシャル プロファイルで、デバイスの HTTP クレデンシャルを確認し再入力する。
Cisco Prime Collaboration リリース 11.1 以前の場合 MSI		
Failed to access MSI.	クレデンシャル プロファイルに入力された MSI クレデンシャルが正しくない。	デバイスの MSI クレデンシャルを確認し、クレデンシャル プロファイルに再入力する。

デバイス クレデンシャル プロファイルの削除

未使用のクレデンシャル プロファイルのみを削除できます。Cisco Prime Collaboration Assurance アプリケーションで管理されているデバイスのクレデンシャルプロファイルを削除しないことを推奨します。

クレデンシャル プロファイルを削除するには、次の手順を実行します。

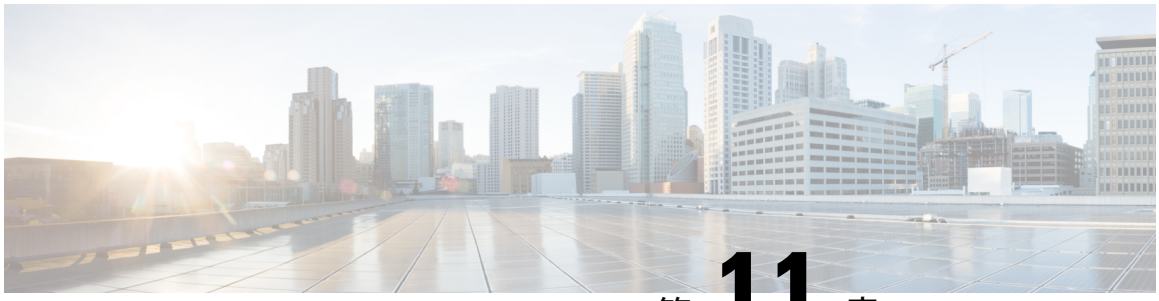
ステップ 1 選択 **[デバイスインベントリ（Device Inventory）]** > **[インベントリ管理（Inventory Management）]**。

Cisco Prime Collaboration リリース 11.5 以降の場合

移行方法 **[インベントリ（Inventory）]** > **[インベントリ管理（Inventory Management）]**

ステップ 2 [Inventory Management] ページで、[Manage Credentials] をクリックします。デフォルトでは、リスト上で最初に表示されるデバイスのクレデンシャルが表示されます。

ステップ 3 プロファイル名を選択し、[削除（Delete）] をクリックします。



第 11 章

クラスタのセットアップ

この項の内容は次のとおりです。

- クラスタのセットアップ （125 ページ）

クラスタのセットアップ

Cisco Prime Collaboration Assurance は、次のクラスタを管理します。

- Cisco TMS
- Cisco VCS
- Cisco Unified CM

ネットワーク内で複数の Cisco TelePresence Management Suite（TMS）を使用している場合は、クラスタ内でこれらのアプリケーションを設定して、Cisco Prime Collaboration Assurance アプリケーションが管理できるようにする必要があります。つまり、Cisco Prime Collaboration Assurance は 2 つのスタンドアロン型 TMS を管理できないということです。

Cisco Prime Collaboration Assurance は、アプリケーション サーバのみを監視します。データベース インスタンスはモニタしません。クラスタ内のすべての Cisco TMS アプリケーション サーバに対して状態ポーリングが実行されます。

TMS クラスタの場合、会議の詳細は、[クラスタの管理（Manage Clusters）] ページで定義されたプライマリ Cisco TMS からインポートされます。

Cisco Prime Collaboration Assurance を MSP モードで導入した場合は、CTX クラスタも管理できます。Cisco Prime Collaboration Assurance は、複数の CTX クラスタを管理できません。クラスタ内の CTX 管理サーバに対して状態ポーリングが実行されます。CTX クラスタの場合、セッションの詳細はプライマリ管理サーバからインポートされます。

Cisco TelePresence Manager、Cisco TMS クラスタ

Cisco TelePresence Manager、Cisco TMSクラスタを検出する前に、クラスタの詳細を [クラスタの管理（Manage Cluster）] ページに入力する必要があります。Cisco TelePresence Manager または Cisco TMS の検出中に、Cisco Prime Collaboration Assurance は、クラスタの詳細とデバイス

のクレデンシャルを使用し（**[デバイスインベントリ（Device Inventory）] > [インベントリ管理（Inventory Management）] > [クレデンシャルの管理（Manage Credentials）]**）、管理アプリケーションを検出します。

（注） CTX クラスタを追加するには、プライマリ CTX 管理サーバに API ロールを持つ新しいユーザを作成してください。この手順の詳細については、「Prime Collaboration Assurance 用のデバイスをセットアップ」のページを参照してください。

Cisco Prime Collaboration リリース 11.5 以降の場合

（注） Cisco TelePresence Manager と Cisco TelePresence Exchange（CTX）クラスタはサポートされていません。

Cisco TMS クラスタを検出する前に、[クラスタの管理（Manage Cluster）] ページでクラスタの詳細を入力する必要があります。Cisco TMS の検出中に、Cisco Prime Collaboration Assurance は、クラスタの詳細とデバイスのクレデンシャルを使用し（**[インベントリ（Inventory）] > [インベントリ管理（Inventory management）] > [クレデンシャルの管理（Manage Credentials）]**）、管理アプリケーションを検出します。

Cisco TMSのクラスタを管理するには、次のようにします。

ステップ 1 選択 **[デバイスインベントリ（Device Inventory）] > [インベントリ管理（Inventory Management）]**。

Cisco Prime Collaboration リリース 11.5 以降の場合

移行方法 **[インベントリ（Inventory）] > [インベントリ管理（Inventory Management）]**

ステップ 2 [インベントリの管理（Inventory Management）] ページで、[CTS-MAN/TMS クラスタの管理（Manage CTS-MAN/TMS Cluster）] をクリックします。

Cisco Prime Collaboration Assurance を MSP モードで展開した場合は、[CTS-MAN/TMS クラスタの管理（Manage CTS-MAN/TMS Cluster）] をクリックします。

Cisco Prime Collaboration リリース 11.5 以降の場合

[インベントリの管理（Inventory Management）] ページで、[TMS クラスタの管理（Manage TMS Cluster）] をクリックします。

Cisco Prime Collaboration Assurance を MSP モードで展開した場合は、**[TMS クラスタの管理（Manage TMS Clusters）]** をクリックします。

ステップ 3 [クラスタの管理（Manage Cluster）] ウィンドウでクラスタ名を入力し、[クラスタタイプ（Cluster Type）] ドロップダウンリストから項目を選択します。

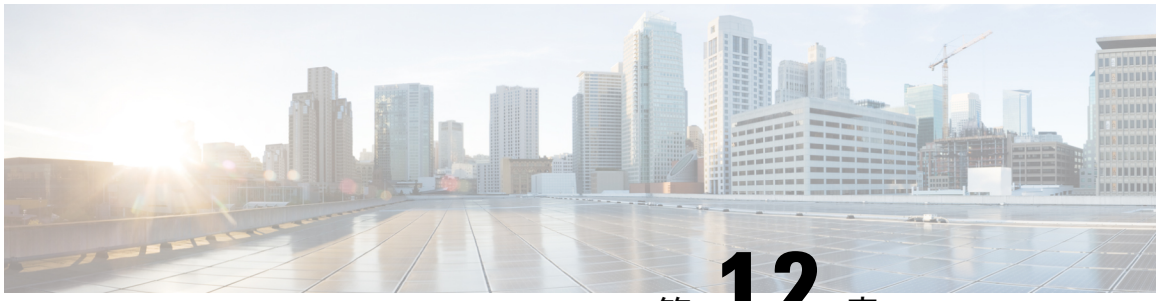
ステップ 4 TMS クラスタの場合は、プライマリ アクティブ サーバ、セカンダリ アクティブ サーバ、またはパッシブ サーバの IP アドレスを入力します。

Cisco Prime Collaboration リリース 11.5 以降の場合

TMS クラスタの場合は、プライマリ アクティブ サーバ、セカンダリ アクティブ サーバ、またはパッシブ サーバの IP アドレスを入力します。

ステップ 5 [追加（Add）] をクリックして、新しいクラスタを追加します。

これらのクラスタを検出するための論理検出を実行します。論理検出の詳細については、「検出方法」を参照してください。ネットワークで初めてクラスタを検出する際に、CTS-MAN と TMS のクラスタに対して、プライマリ、セカンダリ、ホット スタンバイ、およびロードバランサ サーバの詳細を入力できます。後でインベントリの更新や再検出を行う際は、CTS-MAN と TMS クラスタのプライマリ サーバの詳細を入力するだけで済みます。



第 12 章

デバイスの検出

このセクションでは、次の点について説明します。

- デバイスの検出 （129 ページ）

デバイスの検出

Cisco Prime Collaboration Assurance データベースでデバイスを管理するには、検出を実行する必要があります。必要なデバイス クレデンシャルを追加すると、すべてのサポートされるデバイスを Cisco Prime Collaboration Assurance で検出し管理できます。

ライフ サイクルの検出

検出には、次の 3 つのフェーズがあります。

- アクセスレベルの検出：Cisco Prime Collaboration Assurance によって次のことが行われます。

1. デバイスに対し ICMP を使用して ping を実行できるかどうかのチェックが行われます。ICMP がデバイスで有効になっていない場合は、デバイスは [Unreachable] 状態に移行されます。ICMP 検証を無効にする方法については、「デバイスの再検出」を参照してください。
2. IP アドレスに基づいて、定義済みのクレデンシャル プロファイルがすべて取得されます。クレデンシャル プロファイルの定義方法については、デバイス クレデンシャルの管理 （99 ページ）を参照してください。
3. SNMP クレデンシャルが一致しているかどうかのチェックが行われます。
4. デバイスのタイプが特定されます。
5. デバイスのタイプに基づいて、その他すべての必須デバイス クレデンシャルが検査されます。必須クレデンシャルが定義されていない場合、検出は失敗します。必要なデバイス クレデンシャルについては、デバイス クレデンシャルの管理 （99 ページ）を参照してください。

- インベントリの検出：Cisco Prime Collaboration Assurance によって、MIB-II とその他のデバイスの MIB をポーリングし、インベントリ、近接スイッチ、デフォルト ゲートウェイの情報を収集します。また、ポーリングされたデバイスが Cisco Prime Collaboration Assurance でサポートされるかどうかも確認します。
- パス トレース検出：Cisco Prime Collaboration Assurance は、デバイスで CDP が有効になっているかどうかを確認し、CDP に基づいてトポロジを検出します。デバイス間のリンクは CDP を使用して計算され、Cisco Prime Collaboration Assurance データベースに保持されます。

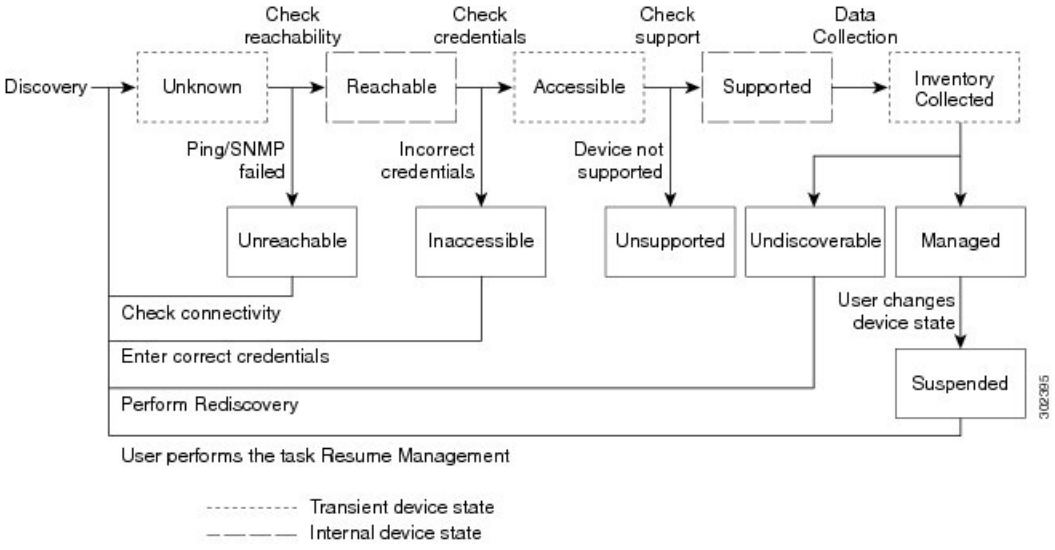
  Cisco Prime Collaboration リリース 11.1 以前の場合

  Cisco Prime Collaboration Assurance が、レイヤ 2 およびレイヤ 3 の両方のパスを検出します。レイヤ 3 パスは、トラブルシューティング ワークフローが手動あるいは自動で起動されると検出されます。デフォルトのホップ カウントは 2 で、設定はできません。

デバイス状態は、Cisco Prime Collaboration Assurance がデバイスにアクセスしてインベントリを収集できることを示しています。デバイスの状態は、ディスカバリまたはインベントリの更新タスクのいずれかを実行した後に限り更新されます。

次の図に、デバイス ディスカバリのライフサイクルを示します。

図 *2:* デバイス検出のライフサイクル



Cisco Prime Collaboration Assurance には、次のデバイス状態が表示されます。

表 *14:* ディスカバリ状態

ディスカバリ状態	説明
不明	これは、デバイスが最初に追加される際の準備中の状態です。これは一時的なステートです。

ディスカバリ状態	説明
Unreachable	Cisco Prime Collaboration Assuranc は、ICMP を使用してデバイスに ping できません。ICMP がデバイスで有効になっていない場合は、デバイスは [Unreachable] 状態に移行されます。
Unsupported	Cisco Prime Collaboration Assurance は、デバイスをデバイス カタログと比較します。デバイスがデバイス カタログのデバイスに一致しないか、SysObjectID が不明の場合、デバイスはこの状態に移行されます。
アクセス可	Cisco Prime Collaboration Assurance は、要求されたすべてのクレデンシャルからデバイスにアクセスできます。これは、アクセス レベル検出の一部であり、デバイス検出中の中間（一時的）状態です。
アクセス不可	Cisco Prime Collaboration Assurance は、要求されたいずれのクレデンシャルからもデバイスにアクセスできません。デバイス クレデンシャルの管理 （99 ページ）を参照してください。クレデンシャルを確認して、デバイスを検出する必要があります。
インベントリ収集	Cisco Prime Collaboration Assurance は、要求されたデータ コレクタを使用して必要なデータを収集できます。これはインベントリ検出の一部であり、デバイス検出中の中間（一時的）状態です。
Undiscoverable	Cisco Prime Collaboration Assurance は、要求されたデータ コレクタを使用して必要なデータを収集できません。デバイスの状態は、次の場合に検出不能になります。 • SNMP や HTTP/HTTPS のタイムアウトが原因で、接続性の問題が発生する場合があります。また、HTTP/HTTPS を使用してデータを収集する場合は、一度に 1 人の HTTP/HTTPS ユーザだけがログインできます。Cisco Prime Collaboration Assurance にこれらの問題のいずれかが存在する場合、デバイス状態は [検出不能（Undiscoverable）] 状態に移行します。再検出を実行する必要があります。 • Cisco Unified CM、CTS、CTMS、およびその他のネットワーク デバイスには、収集が必要なデータはありません。 • SNMP や HTTP/HTTPS のタイムアウトが原因で、接続性の問題が発生する場合があります。また、HTTP/HTTPS を使用してデータを収集する場合は、一度に 1 人の HTTP/HTTPS ユーザだけがログインできます。Cisco Prime Collaboration Assurance にこれらの問題のいずれかが存在する場合、デバイス状態は [検出不能（Undiscoverable）] 状態に移行します。再検出を実行する必要があります。

ディスカバリ状態	説明
Managed	Cisco Prime Collaboration Assurance により、必要なデバイス データがインベントリ データベースに正常にインポートされました。この状態のデバイスでは、すべての会議、エンドポイント、およびインベントリ データを使用できます。 **Cisco Prime Collaboration リリース 11.1 以前の場合** この状態になっているデバイスだけをトラブルシューティングできます。 （注） Cisco Prime Collaboration Assurance はサードパーティ デバイスをサポートしますが、その管理性は MIB-II サポートに依存します。 Cisco Prime Collaboration Assurance のインベントリがデバイスの制限を超えた場合は、警告メッセージが表示されます。Cisco Prime Collaboration Assurance で管理可能なデバイス数については、『Cisco Prime Collaboration Assurance and Analytics インストールおよびアップグレード ガイド』を参照してください。
Partially Managed	管理対象状態にあるものの、一部のクレデンシャルが不足しているデバイスの数。これらのクレデンシャルは、インベントリの管理に必須ではありませんが、会議のモニタリングなど、他のすべての機能に必要です。対応する数をクリックすると、インベントリ テーブルをクロス起動して、管理対象でありながらクレデンシャルが不足しているすべてのデバイスの一覧を確認できます。この数は、クレデンシャルの追加後に再検出を実行した場合にのみ更新されます。
Suspended	ユーザがデバイスのモニタリングを一時停止しています。この状態のデバイスでは、会議とエンドポイント データは表示されません。この状態のデバイスでは、定期的なポーリングも実行されません。これらのデバイスのインベントリは更新できません。これを行うには、[Resume Management] を実行する必要があります。

（注） 不明なエンドポイントがクラスタ内の登録済み状態に移行すると、[エンドポイントの診断（Endpoint Diagnostics）] ページに、同じエンドポイントのデュアル エントリ（不明および登録済み状態）が午前0時まで表示されます。登録済み状態にあるエンドポイントの単一のエントリは、毎晩行われるクラスタの検出後にのみ表示できます。

関連トピック

デバイス クレデンシャルの管理
デバイス クレデンシャル プロファイルの追加 （100 ページ）
[Credential Profiles] のフィールドの説明

管理対象デバイスの一時停止と再開 （223 ページ）

Cisco Prime Collaboration Assurance の削除時にデバイスを削除

デバイスと関連付けられたエンドポイントは、**[State（状態）]** が **[削除済み（Deleted）]** の場合、データベースには保持されません。

下の表は、削除されるデバイスと関連デバイスの一覧表示です。

デバイス	削除される関連デバイス
CUCM の削除： **1.** パブリッシャ **2.** サブスクライバ	関連デバイスは、次のとおりです **1.** クラスタに関連付けられているすべてのものを削除します。 **2.** サブスクライバとこれに登録されているエンドポイントを削除します。
CME の削除	CME とこれに登録されているエンドポイントを削除します。
VCS の削除	これに登録されているすべてのエンドポイントを削除します。
TMS の削除	TMS のみが削除され、MCU、TP_Conductor などの関連デバイスは削除されません。
ESX の削除	すべてのホストされた VM ノードを削除します。
VCENTER の削除	VCENTER が管理するすべての ESX デバイスと関連付けられているノードを削除します。
TP、UNITY CONNECTION、MULTIPOINT CONTROLLER、IM&P、その他のインフラストラクチャ デバイスの削除	デバイスのみが削除されます。

検出方法

次のいずれかの検出方法を選択して、Cisco Prime Collaboration Assurance のデバイスを管理します。

Cisco Prime Collaboration リリース 11.1 以前の場合

検索タイプ	検出方法	説明

自動検出	論理検出	• 管理アプリケーション、会議デバイス、ならびに、Cisco TMS、Cisco VCS、Cisco Unified CM などのコール プロセッサを検出します。
		• 、Cisco TMS、Cisco Unified CM、Cisco VCS に登録されているすべてのエンドポイントとインフラストラクチャ デバイスは、論理検出の際に自動的に検出されます。
		  • Cisco C および Ex シリーズの TelePresence システムの場合、Cisco Prime Collaboration Assurance はファースト ホップ ルータとスイッチを検出しません。
		  • Cisco TMS の論理検出は、VCS、コーデック、Cisco MCU、TPS、Cisco IP Video Phone E20、Cisco MXP シリーズを検出します。
		• Cisco Unified CM Publisher の論理検出は、ネットワーク内にあるその他の Cisco Unified CM（サブスクライバ）、Cisco Unity、Cisco MGCP Voice Gateway、H.323 Voice Gateway、Gatekeeper、CTI アプリケーションを検出します。
		• Cisco Unified CM の SIP デバイス用の論理検出には、コンダクタの検出が含まれています。SIP が設定済みのコンダクタ IP では SNMP が有効ではないため、Cisco Prime Collaboration Assurance では管理されません。このような設定では、Cisco Unified CM の論理検出を実行する前に、管理者 IP を持つコンダクタを管理する必要があります。
		• 管理アプリケーション、会議デバイス、コール プロセッサのどれにも登録されていないエンドポイントとインフラストラクチャ デバイスは、論理検出を使用して検出することはできません。これらのデバイスを検出するには、ping スイープまたは直接検出を使用します。
		• Cisco CTX クラスタは、論理検出を使用して検出されます。
		• Unified Contact Center デバイスは、論理検出を使用して検出されます。
		• 論理検出は、論理的にシード デバイスまたはクラスタに関連付けられている場合は、削除されたデバイスを再度検出します。

検索タイプ	検出方法	説明
自動検出	CDP	• 使用されているメディアやプロトコルとは関係なくデバイスを検出します。このプロトコルは、すべてのシスコ製の機器（ルータ、アクセス サーバ、ブリッジ、スイッチなど）で実行されます。 • この検出方法はネイバーデバイスを見つけるのにCDPネイバーテーブルを照会します。CDP がイネーブルに設定されている場合、検出はSNMP経由で各シードデバイス（およびそのピア）のCDPキャッシュを照会します。CDP検出の後で、論理検出が自動的に実行されます。つまり、コール プロセッサまたは管理デバイスがCDP検出で検出された場合は、そのデバイスに登録されているすべてのエンドポイントとインフラストラクチャ デバイスも検出されます。 • CDP検出を実行するには、デバイス上でCDPがイネーブルに設定されている必要があります。 • CDP検索に使用可能なシードデバイス数に制限はありません。ただし、大規模なネットワークの場合は、一度にすべてのシードデバイスではなく、限られた数のシードデバイスで検索を実行するよう推奨します。

検索タイプ	検出方法	説明
自動検出	Ping Sweep	• 指定の IP アドレスとサブネット マスクの組み合わせから、IP アドレスの範囲内でデバイスを検出します。 • この方法では、デバイスの到達可能性を調べるために、範囲内の各 IP アドレスに ping が送信されます。デバイスが到達可能である場合は、ping するサブネットおよびネットワーク マスクのリストを管理者が指定する必要があります。ping スイープ検出の後で、論理検出が自動的に実行されます。つまり、コール プロセッサまたは管理デバイスが ping スイープ検出で検出された場合は、そのデバイスに登録されているすべてのエンドポイントとインフラストラクチャ デバイスも検出されます。 • コール プロセッサが展開されていない場合、またはデバイスが 1 つもコールプロセッサに登録されていない場合は、ping スイープ検出を使用します。この方法では、ターゲット ネットワーク内のすべての新しいインフラストラクチャデバイス、新しいネットワーク デバイス、およびデバイスの新しい位置が検出されます。ターゲット ネットワークのサブネットおよびネットワーク マスクのリストを指定する必要があります。スケジュールされた ping スイープ検出中に、ネットワーク内のすべてのデバイスが特定されて、一致するクレデンシャル プロファイルが検索されます。新しいデバイスが検出された場合は、そのデバイスがインベントリに追加されます。 • ping スイープ検出では、シード デバイスは必要はありません。代わりに、ping するサブネットおよびネットワーク マスクのリストを指定する必要があります。 • IP 範囲が大きい場合、Ping スイープ検出には通常よりも時間がかかることがあります。 • Ping スイープ および CDP 検出を実行するには、クレデンシャル プロファイルを作成する必要があります。 • Ping スイープは、IPv6 アドレスを持つデバイスでは機能しません。

検索タイプ	検出方法	説明
-	Add Devices	• IP アドレスを使用してデバイスを直接検出します。 • ネットワーク内の個々のデバイスを検出します。 • スケジュール設定された検索中に間違ったクレデンシャルが原因でデバイスの検出が失敗した場合は、ダイレクト検出方法を使用して、エラーが発生したデバイスのみを検出できます。 • 論理検出を使用して、SIP デバイスや Presence サーバを検出することはできません。これらのデバイスを手動で追加するか、直接検出を実行する必要があります。 • 登録されているネットワーク デバイスやビデオエンドポイントを検出せずに、シードまたはパブリッシャのデバイスを検出します。 • 新規インストールの後に検出されていない、インフラストラクチャ デバイスを検出します。 • MSP モードの場合、ネットワーク デバイスを自動検出せずに 1 台のデバイスを検出します。
-	インポート	このオプションを使用して、次のものを追加します。 • 大量のデバイス。 • 大規模なグループのサブネット内から、デバイスのサブセット。

（注）
- CDP、Ping スイープ、追加、またはインポートのいずれかの方法を使用してエンドポイントを検出する場合は、エンドポイントが登録されている、当該の Unified CM または Cisco VCS が再検出されていることを確認します。エンドポイントは、コール コントローラに関連付けられている必要があります。
- MSP モードの場合、-ネットワーク デバイスを自動検出せずに 1 台のデバイスを検出するには、デバイスの [追加（Add）] または [インポート（Import）] オプションを使用します。

Cisco Prime Collaboration リリース 11.5 以降の場合

検索タイプ	Discover	説明
自動検出	Communications Manager（UCM）および接続されたデバイス	• 次のパスを使用して、Cisco Unified CM の論理検出を実行します。 **[Inventory（インベントリ）]** > **[インベントリ管理（Inventory Management）]** > **[自動検出（Auto Discovery）]** パス（Path） • Cisco Unified CM に登録されているすべてのエンドポイントとインフラストラク チャデバイスは、検出中に自動検出されます。 • コール プロセッサに登録されていないエンドポイントおよびインフラストラクチャ デバイスは、論理検出を使用して検出することはできません。これらのデバイスを検出するには、ping スイープまたは直接検出を使用します。 • Communications Manager とここに接続したデバイスがシードデバイスまたはクラスタに関連付けられている場合、削除されたデバイスを再度検出します。 • Cisco Unified CM Publisher の論理検出は、ネットワーク内にあるその他の Cisco Unified CM（サブスクライバ）、Cisco MGCP Voice Gateway、H.323 Voice Gateway、Gatekeeper、CTI アプリケーションを検出します。 • Cisco Unified CM の SIP デバイス用の論理検出には、コンダクタの検出が含まれています。SIP が設定済みのコンダクタ IP では SNMP が有効ではないため、Cisco Prime Collaboration Assurance では管理されません。このような設定では、Cisco Unified CM の論理検出を実行する前に、管理者 IP を持つコンダクタを管理する必要があります。 • CUCM の論理検出（Communications Manager Publisher）では、SIP トランクは検出されません。 • MSP モードでは、パブリッシャ用のお客様の名前を変更する場合は、そのクラスタに含まれる他のすべてのインフラストラクチャ デバイスで新しいお客様の名前に更新します。 • Unified Communications Manager()を自動的に検出する場合 **[Inventory（インベントリ）]** > **[インベントリ管理（Inventory Management）]** > **[自動検出（Auto Discovery）][自動設定（Auto-Configuration）]** オプションを使用して、Unified Communications Manager servers の CDR 課金アプリケーション サーバおよび syslog レシーバとして Cisco Prime Collaboration Assurance サーバを追加できます。
		Video Communications Server（VCS）、Expressway クラスタ、接続されたデバイスの論理検出を実行します。

検索タイプ	Discover	説明
	Video Communications Server（VCS）/ Expressway クラスタおよび接続されたデバイス	
	Telepresence Management Suite（TMS）および接続されたデバイス	Telepresence Management Suite（(TMS）と接続されたデバイスの論理検出を実行します。 Cisco TMS の論理検出は、、Cisco MCU、TPS、TP コンダクタを検出します。
	Contact Center Customer Voice Portal（CVP）および接続されたデバイス	Contact Center Customer Voice Portal（CVP）および接続されたデバイスの論理検出を実行します。
	VCenter および接続された ESXi デバイス	VCenter および接続された ESXi デバイスの論理検出を実行します。 Cisco C および EX シリーズの TelePresence システムの場合、Cisco Prime Collaboration Assurance はファーストホップルータとスイッチを検出しません。
	UCS Manager	UCS Manager の論理検出を実行します。

検索タイプ	Discover	説明
自動検出	CDP を使用したネットワーク デバイス	• 使用されているメディアやプロトコルとは関係なくデバイスを検出します。このプロトコルは、すべてのシスコ製の機器（ルータ、アクセス サーバ、ブリッジ、スイッチなど）で実行されます。 • この検出方法はネイバー デバイスを見つけるのに CDP ネイバー テーブルを照会します。CDP が有効な場合、検出は SNMP を使用して各シード デバイス（およびそのピア）の CDP キャッシュを照会します。CDP 検出の後で、論理検出が自動的に実行されます。つまり、コール プロセッサまたは管理デバイスが CDP 検出で検出された場合は、そのデバイスに登録されているすべてのエンドポイントとインフラストラクチャ デバイスも検出されます。 • CDP 検出を実行するには、デバイス上で CDP がイネーブルに設定されている必要があります。 • CDP 検索に使用可能なシード デバイス数に制限はありません。ただし、大規模なネットワークの場合は、一度にすべてのシード デバイスではなく、限られた数のシード デバイスで検索を実行するよう推奨します。

検索タイプ	Discover	説明
自動検出	Ping を使用したネットワークデバイス	• 指定の IP アドレスとサブネット マスクの組み合わせから、IP アドレスの範囲内でデバイスを検出します。 • この方法では、デバイスの可用性を調べるために、範囲内の各 IP アドレスに ping が送信されます。デバイスが到達可能である場合は、ping するサブネットおよびネットワーク マスクのリストを管理者が指定する必要があります。ping スイープ検出の後で、論理検出が自動的に実行されます。つまり、コール プロセッサまたは管理デバイスが ping スイープ検出で検出された場合は、そのデバイスに登録されているすべてのエンドポイントとインフラストラクチャ デバイスも検出されます。 • コール プロセッサが展開されていない場合、またはデバイスが 1 つもコール プロセッサに登録されていない場合は、ping スイープ検出を使用します。この方法では、ターゲット ネットワーク内のすべての新しいインフラストラクチャ デバイス、新しいネットワーク デバイス、およびデバイスの新しい位置が検出されます。ターゲット ネットワークのサブネットおよびネットワーク マスクのリストを指定する必要があります。スケジュールされた ping スイープ検出中に、ネットワーク内のすべてのデバイスが特定されて、一致するクレデンシャル プロファイルが検索されます。新しいデバイスが検出された場合は、そのデバイスがインベントリに追加されます。 • ping スイープ検出では、シード デバイスは必要はありません。代わりに、ping するサブネットおよびネットワーク マスクのリストを指定する必要があります。 • IP 範囲が大きい場合、Ping スイープ検出には通常よりも時間がかかることがあります。 • Ping スイープ および CDP 検出を実行するには、クレデンシャル プロファイルを作成する必要があります。 • Ping スイープは、IPv6 アドレスを持つデバイスでは機能しません。
自動検出	任意のデバイス	コンダクタなどのその他のすべてのシード デバイスを検出します。

検索タイプ	Discover	説明
-	Add Devices	• IP アドレスを使用してデバイスを直接検出します。 • ネットワーク内の個々のデバイスを検出します。 • スケジュール設定された検索中に間違ったクレデンシャルが原因でデバイスの検出が失敗した場合は、ダイレクト検出方法を使用して、エラーが発生したデバイスのみを検出できます。 • 論理検出を使用して、SIP デバイスや Presence サーバを検出することはできません。これらのデバイスを手動で追加するか、直接検出を実行する必要があります。 • 登録されているネットワーク デバイスやビデオ エンドポイントを検出せずに、シードまたはパブリッシャのデバイスを検出します。 • 新規インストールの後に検出されていない、インフラストラクチャ デバイスを検出します。 • MSP モードの場合、ネットワーク デバイスを自動検出せずに 1 台のデバイスを検出します。
-	インポート	このオプションを使用して、次のものを追加します。 • 大量のデバイス。 • 大規模なグループのサブネット内から、デバイスのサブセット。

（注） 管理アプリケーション、会議デバイス、コールプロセッサのどれにも登録されていないエンドポイントとインフラストラクチャ デバイスは、論理検出を使用して検出することはできません。これらのデバイスを検出するには、ping スイープまたは直接検出を使用します。

前提条件と推奨事項

検出を実行する前には次の点を確認し、必要に応じてデバイスを設定する必要があります。

すべてのデバイス

- デバイスに DNS が設定されている場合、Cisco Prime Collaboration Assurance がそのデバイスの DNS 名を解決できることを確認します。DNS サーバの設定が正しいことを確認します。これは、Cisco Unified CM、Unified Presence サーバ、Unity Connection デバイスではとても重要です。Cisco Prime Collaboration Assurance は、MGCP ゲートウェイのホスト名を解決する必要があります。これは、通常、MGCP ゲートウェイのホス

ト名はゲートウェイとして DNS サーバに追加されず、Cisco Unified CM は DNS を解決せずに同時に操作することが可能なためです。ただし、Cisco Unified CM は MGCP ゲートウェイのホスト名を FQDN として捉えるため、解決することはできません。

- パブリッシャ名とホスト名は一致する必要があります（大文字と小文字を区別）。
- CDP は、すべての 、CTMS、ネットワーク デバイス（ルータとスイッチ）で有効にする必要があります。詳細については、「Cisco IOS を実行する Cisco ルータとスイッチで Cisco Discovery Protocol を設定」を参照してください。
- およびIP フォン/ソフトウェア クライアントを除くエンドポイントやTelePresence サーバなどのデバイスは、個別に検出することができます。これらのエンドポイントは、登録されているコール プロセッサの検出を介してのみ検出されます。
- 入力したデバイスのクレデンシャルが正しいことを確認する必要があります。検出プロセス中、検出するデバイスに基づき Cisco Prime Collaboration Assurance は、CLI、HTTP/HTTPS、SNMP を使用してデバイスに接続します。
- デバイスを追加するときは、HTTP（および HTTPS）ポート番号はオプションです。これらの設定は自動的に削除されます。
- 音声とビデオの両方のエンドポイントがネットワーク内に導入されている場合は、検出に時間がかかるため、ネットワーク内のすべてのクラスタを同時に検出することはありません。
- ファイアウォール デバイスはサポートされていません。
- HTTP を使用してデバイスの詳細を取得する場合は、HTTP ファイアウォールを無効にします。
- HSRP 対応デバイスはサポートされていません。
- 複数のインターフェイスと HTTP 管理アクセスを備えたデバイスを追加する場合は、HTTP 管理者アクセスを有効にしたもののと同じインターフェイスを使用し、Cisco Prime Collaboration Assurance でデバイスを管理する必要があります。
- デバイスの検出後、ネットワーク デバイスやインフラストラクチャ デバイス（、CTMS、Cisco Unified CM、Cisco MCU、Cisco VCS、Cisco TS など）の IP アドレスが変更された場合は、新しい IP アドレスまたはホスト名を指定して、これらのデバイスを再検出する必要があります。デバイスの再検出の詳細については、デバイスの再検出 （168 ページ）を参照してください。
- 管理対象デバイスがネットワークから取り外された場合は、そのデバイスは到達不能でも、次のインベントリの収集が行われるまで [Managed] 状態のままとなります。デバイスに到達できない場合は、このデバイスに対して到達不可能のイベントが発生します。
- デバイスで設定を変更した場合、Cisco Prime Collaboration Assurance はインベントリ収集プロセスのみでデバイスを検出することができます。したがって、デバイスで変更された設定は、Cisco Prime Collaboration Assurance が設定の変更後に次のインベントリ コレクションを行うまで表示されません。

- インベントリを定期的に更新し、Cisco Prime Collaboration Assurance データベースと同期させるには、インベントリの更新を実行する必要があります。詳細については、インベントリ詳細の更新と収集を参照してください。

Cisco Unified CM

- Cisco Prime Collaboration Assurance は、Unified Communications Manager のクラスタ検出をサポートしています。クラスタ ID は一意である必要があります。
- Unified Communications Manager の Access Control List（ACL）には、管理するすべてのエンドポイントが含まれている必要があります。Unified Communications Manager の SNMP ユーザ設定に ACL が含まれている場合、クラスタ内のすべての Unified Communications Manager ノードには、Cisco Prime Collaboration Assurance サーバの IP アドレスが含まれている必要があります。
- Cisco Prime Collaboration Assurance は、クラスタを管理するため、Unified Communications Manager パブリッシャのみを検出して管理する必要があります。サブスクライバが直接検出されることはなく、パブリッシャによって検出されます。Cisco Prime Collaboration Assurance では、パブリッシャを管理してクラスタを監視する必要があります。Computer Telephony Integration（CTI）サービスは、すべてのサブスクライバで実行されている必要があります。Unified Communications Manager のアクセス制御リストには、管理の必要があるすべてのエンドポイントが含まれていることを確認します。Unified Communications Manager の SNMP ユーザ設定にアクセス制御リストの使用が含まれている場合、Unified Communications Manager サーバの IP アドレスをクラスタ内の Unified Communications Manager ノードに入力する必要があります。
- Cisco Prime Collaboration Assurance には、適切な IP アドレス パターンを使用して、ELM または PLM デバイス タイプのクレデンシャルプロファイルを提供する必要があります。これにより、自動検出ユーザインターフェイスを使用して Unified Communications Manager パブリッシャが Cisco Prime Collaboration Assurance に追加された場合、設定した ELM または PLM が検出されて管理されます。

  Unified Communications Manager が Cisco Prime Collaboration Assurance（**[Inventory（インベントリ）]**>**[インベントリ管理（Inventory Management）]**>**[自動検出（Auto Discovery）]** で自動検出されると、自動設定オプションを使用して、Unified Communications Manager 内の syslog レシーバや CDR 課金アプリケーション サーバを自動に設定することができます。Syslog レシーバや CDR 課金アプリケーション サーバを手動で設定する場合は、[自動設定（Auto-Configuration）] オプションの下にあるチェックボックスをオフにします。Syslog レシーバまたは CDR 課金アプリケーション サーバのエントリを手動で追加する場合は、Unified Communications Manager のスロットに空きがあるかどうか確認することを推奨します。

（注） Syslog レシーバや CDR 課金アプリケーション サーバは、Unified Communications Manager が Cisco Prime Collaboration Assurance 管理されている状態にある場合のみ、自動に設定することができます。

PLM は、別のグループとして、Cisco Unified Communications（UC）アプリケーションの下で表示できます。

- JTAPI クレデンシャルは、Cisco Unified CM クラスタの場合は任意です。ただし、SNMP および HTTP クレデンシャルは Cisco Unified CM パブリッシャおよびサブスクライバに必須です。
- Cisco Unified CM の検出後に新しいエンドポイントを登録した場合は、Unified CM Publisher ノードを再検出して Cisco Prime Collaboration Assurance に追加する必要があります。デバイスの再検出の詳細については、デバイスの再検出（168 ページ）を参照してください。

（注） 手動によるサブスクライブ ノードの追加は推奨されません。

Cisco Prime Collaboration リリース 11.5 以前の場合

MSP モードでは、Cisco Unified CM の検出前に新しいエンドポイントを登録した場合は、そのエンドポイントを削除し、Cisco Unified CM の検出後に再度追加する必要があります。

Cisco Unified CM Express および Cisco Unity Express

- Cisco Cius と Cisco Unified IP Phone 8900 および 9900 シリーズの検出では、これらのデバイスがインベントリ テーブルに表示されるよう、HTTP インターフェイスを有効にする必要があります。詳細については、『Cisco Unified Communications Manager 7.1 (3) (SIP) 用の Cisco Unified IP Phone 8961、9951、9971 管理ガイド』の 「「Web ページ アクセスの有効化と無効化」」セクションを参照してください。
- Cisco Prime Collaboration Assurance を有効にし、Cisco Unified CM Express と Cisco Unity Express（CUE）で正しい電話番号を提供するには、次の設定を使用する必要があります。

  ```
  ephone 8 mac-address 001A。E2BC.3EFB タイプ 7945
  ```

  type は、電話機のモデル タイプです。モデル タイプが不明な場合は、Cisco.com ですべての電話機モデル タイプについて確認するか、type ? と入力します。電話数を表示させる方法の詳細については、 および [インベントリ管理（Inventory Management）] ページにある および [デバイス管理の概要（Device Management Summary）] ウィンドウを参照してください。
- UC500 シリーズ ルータが Cisco Unified CM Express を実行している場合は、各電話機の設定で「type」を設定し、CISCO-CME_MIB の cmeEphoneModel MIB 変数が正しい電話機モデルを返す必要があります。これにより、Cisco Prime Collaboration Assurance は、Cisco Unified CM Express に登録された電話機を検出できます。
- Cisco Unified CM Express に接続されている Cisco Unity Express が Service Level View に表示されるようにするには、次の設定を使用する必要があります。

  ```
  ダイヤル ピア音声 2999 voip < ここで voip タグ 2999 はボイスメール > 通知先パターン 2105 < プレフィックスと異なる必要があります。設定済みのボイスメール 2105 > の完全な E.164 である必要があります。conference protocol sipv2 conference target ipv4:10.10.1.121
  ```

```
dtmf-relay sip-notify codec g711ulaw no vad ! ! テレフォニーサービスのボイスメール
2105
```

ここで dial-peer VoIP タグ（2999）はボイスメール番号と等しくなく、destination-pattern タグ（2105）はボイスメール番号と等しくなっています。これにより、Unity Express が Service Level View で適切に表示されます。

Cisco VCS および Cisco VCS Expressway

- Cisco VCS クラスタを検出できます。クラスタ名は一意である必要があり、Cisco Prime Collaboration Assurance が管理する必要があるすべてのエンドポイントは、Cisco VCS に登録されている必要があります。VCS の検出中には、登録されているエンドポイントも検出されます。クラスタ内のすべての VCS を必ず管理状態にすることで、会議の監視など、関連するすべての機能が動作せず、CDR の作成に影響しないようにします。

（注） たとえクラスタ内の 1 つの VCS でも管理状態にないと、データレポートに不整合が発生する場合があります。

- Cisco VCS の検出後には、新しく登録されたエンドポイントが自動的に検出されます。また、エンドポイントの IP アドレスを変更すると、Cisco Prime Collaboration Assurance は IP アドレスの変更を自動的に検出します。
- Cisco VCS Expressway が DMZ 内で設定されている場合、Cisco Prime Collaboration Assurance は SNMP を介して Cisco VCS Expressway にアクセスする必要があります。アクセスできない場合、このデバイスは [Inaccessible] 状態になります。Cisco Prime Collaboration Assurance のデバイスの設定についての詳細は、次の場所にあるリストを参照してください。
  - Cisco Prime Collaboration Assurance のデバイス設定
  - Cisco Prime Collaboration Assurance のデバイス設定

Cisco Prime Collaboration リリース 11.1 以前の場合

CTS-Manager

- Cisco Prime Collaboration Assurance のライセンス版をインストールしている場合は、CTS-Manager Reporting API を設定する必要があります。この機能が CTS-Manager 1.7、1.8、または 1.9 に設定されていない場合、Cisco Prime Collaboration Assurance は CTS-Manager を管理しません。詳細については、『Cisco TelePresence Manager Reporting API 開発者ガイド』を参照してください。
- Cisco Prime Collaboration Assurance は、2 つのスタンドアロン型 CTS-Manager を管理できません。複数の CTS-Manager を使用している場合は、Cisco Prime Collaboration Assurance アプリケーション用にクラスタ内で設定して管理する必要があります。検出を実行する前に、プライマリ サーバの IP アドレスとホット スタンバイサーバまたはセカンダリ サーバの詳細を次のページに入力します。 **[デバイス インベントリ**

（**Device Inventory**）] > **[インベントリ管理（Inventory Management）] > [CTS-MAN/TMS/CTX クラスタの管理（Manage CTS-MAN/TMS/CTX Clusters）]**。

Cisco Prime Collaboration リリース 11.1 以前の場合

CTX クラスタ

- Cisco Prime Collaboration Assurance は、Managed Service Provider（MSP）モードのみで Cisco TelePresence Exchange（CTX）クラスタをサポートします。クラスタ名は一意である必要があります。各 CTX クラスタは、1 つのサーバをプライマリ管理サーバ、もう 1 つをセカンダリ サーバとして指名する必要があります。Cisco Prime Collaboration Assurance がクラスタを管理するには、プライマリとセカンダリの管理サーバを検出して管理する必要があります。データベース サーバとコール エンジン サーバは自動的に検出されます。
- 管理ノードでは、API ユーザと SNMP クレデンシャルが必要です。コール エンジンとデータベース ノードでは、SNMP クレデンシャルのみが必要です。詳細については、「Cisco Prime Collaboration Assurance 用のデバイスをセットアップ」を参照してください。
- 検出を実行する前に、プライマリおよびセカンダリ管理サーバの詳細の IP アドレスを次のページに入力します。 。

Cisco TelePresence Conductor

Cisco Prime Collaboration Assurance は、スタンドアロン モデル内で Cisco TelePresence Conductor XC バージョン 1.2 から 3.0.1 をサポートします。クラスタ モデルはサポートしていません。

Cisco TelePresence Management Suite（TMS）の自動検出では、Cisco TelePresence Conductor も検出します。

Cisco TelePresence Conductor は、Cisco Prime Collaboration Assurance サーバのエンタープライズ モードのみでサポートされています。

メディア サーバ

CDP（Cisco Discovery Protocol）がメディア サーバで有効になっていない場合（無効になっているまたは応答しない場合）、Cisco Prime Collaboration Assurance はデバイスを正常に検出することはなく、デバイスは Unsupported 状態へと移行します。

モバイルおよびリモートアクセス（MRA）クライアント

Cisco Jabber、Cisco TelePresence MX シリーズ、Cisco TelePresence System EX シリーズ、Cisco TelePresence System SX シリーズなどのモバイル リモート アクセス（MRA）クライアントは、Cisco Unified Communications Manager の一部としてのみ検出されます。

MRA を正常に検出するには、Cisco Prime Collaboration Assurance で Cisco Expressway のコア機能を搭載した Cisco VCS が Managed 状態にある必要があります。Cisco Expressway のコア機能を搭載した Cisco VCS が Managed 状態にはなく、Cisco Unified Communications Manager が直接検出された場合、[インベントリ管理（Inventory Management）] の では重

複した IP アドレス（Cisco Expressway のコア機能を搭載した Cisco VCS と同じもの）を持つ MRA クライアントが表示されます。

VCS Core が Cisco Prime Collaboration Assurance で管理されていない場合、（インベントリで表示されている）TP MRA エンドポイントは検出されません。

Cisco Unified Contact Center Enterprise（Unified CCE）およびパッケージ化されたContact Center Enterprise（PCCE）

- Cisco Prime Collaboration Assurance は Simple Network Management Protocol（SNMP）機能を使用して、Unified CCE および PCCE デバイスの検出をサポートします。Cisco Prime Collaboration Assurance のデバイスの設定についての詳細は、次の場所にあるリストを参照してください。
  - Cisco Prime Collaboration Assurance のデバイス設定
  - Cisco Prime Collaboration Assurance のデバイス設定
- SNMP エージェントが機能するには、Unified ICM/CCE サーバに Microsoft Windows SNMP コンポーネントをインストールする必要があります。Microsoft Windows SNMP サービスは Web セットアップの一部として無効になっており、SNMP 要求を処理するため、Cisco Contact Center SNMP Management サービスによって置き換えられています。
- Cisco SNMP エージェント管理の設定は、Windows Management Console Snap-in を使用して設定することができます。
- Cisco Prime Collaboration Assurance では、[SNMP Agent Management Snap-in] ウィンドウの下にある **[システムの説明（System Description）]** フィールドに特殊文字を入力すると、認証エラーと間違ったデバイス情報が表示されます。説明にハイフン（-）、二重引用符（"）、アスタリスク（*）、オクトソープ（#）、ドル（$）、アンダースコア（_）、パーセント記号（%）、アンパサンド（&）、バックスラッシュ（\）、山カッコ（<>）、角カッコ（[ ]）を含めることはできません。

Cisco Unified Contact Center Express（Unified CCX）

SNMP を設定する必要があります。Cisco Prime Collaboration Assurance のデバイスの設定についての詳細は、次の場所にあるリストを参照してください。

- Cisco Prime Collaboration Assurance のデバイス設定
- Cisco Prime Collaboration Assurance のデバイス設定

Cisco SocialMiner

SNMP を設定する必要があります。Cisco Prime Collaboration Assurance のデバイスの設定についての詳細は、次の場所にあるリストを参照してください。

- Cisco Prime Collaboration Assurance のデバイス設定
- Cisco Prime Collaboration Assurance のデバイス設定

Cisco Integrated Management Controller（CIMC）

- Cisco Prime Collaboration Assurance は、CIMC デバイス用のアラームとイベントに関するトラップを生成し、トラップの受信者に通知を送信します。トラップは SNMPv1c 通知に変換され、CISCO-UNIFIED-COMPUTING-MIB に従いフォーマットされます。
- システムは CIMC デバイスを自動検出できません。**[デバイスの追加（Add Device）]** ボタンを使用して、デバイスを手動で追加する必要があります。 **[デバイスインベントリ（Device Inventory）]** > **[インベントリ管理（Inventory Management）]**。
- **Cisco Prime Collaboration リリース 11.5 以降の場合**

  システムは CIMC デバイスを自動検出できません。**[デバイスの追加（Add Device）]** ボタンを使用して、デバイスを手動で追加する必要があります。 **[インベントリ（Inventory）]** > **[インベントリ管理（Inventory Management）]**。
- SNMP を設定する必要があります。Cisco Prime Collaboration Assurance のデバイスの設定についての詳細は、次の場所にあるリストを参照してください。
  - Cisco Prime Collaboration Assurance のデバイス設定
  - Cisco Prime Collaboration Assurance のデバイス設定
- CIMC デバイスは、正しい IP アドレスと SNMP クレデンシャルを入力しないと、管理状態には入りません。

Cisco Prime Collaboration リリース 11.5 以降の場合

Cisco Unified Attendant Console

システムは、サードパーティの Windows デバイスとして Cisco Unified Attendant Console をサポートします。Cisco Prime Collaboration Assurance で Cisco Unified Attendant Console をサポートするには、SNMP を設定する必要があります。詳細については、『Cisco Prime Collaboration Assurance のデバイス設定』を参照してください。

Cisco Prime Collaboration リリース 11.6 以降の場合

CE イメージ搭載の ciscoDX70 および ciscoDX80

システムは、CE イメージ搭載の ciscoDX70 および ciscoDX80 デバイスをサポートします。ciscoDX70 および ciscoDX80 デバイスは、Cisco TelePresence デバイスと同様の機能を備えています。Cisco Prime Collaboration Assurance で ciscoDX70 および ciscoDX80 デバイスを検出するには、DX シリーズ デバイスを Cisco Unified Call Manager（UCM）に登録する必要があります。Cisco Prime Collaboration Assuranceで ciscoDX70 および ciscoDX80 デバイスをサポートするには、SNMP、HTTP、CLI を設定する必要があります。詳細については、『Cisco Prime Collaboration Assurance のデバイス設定』を参照してください。

（注） Cisco Prime Collaboration Assurance は、CE イメージ搭載の ciscoDX70 および ciscoDX80 デバイスでは、CMR レポートおよびエンドポイントの診断機能をサポートしません。

デバイスの自動検出

エンドポイントとサブスクライバ デバイスが登録されている場合は、シード デバイスまたはパブリッシャ デバイスを検出できます。

（注）
- 探索ジョブは、いったん開始されると、停止したり取り消したりすることはできません。
- ネットワークで ping スイープと CDP 検出の両方を同時に実行することはできません。

論理検出を使用してクラスタを検出するには、クラスタのパブリッシャを検出する必要があります。これによって自動的に、そのサブスクライバが検出され、パブリッシャとサブスクライバの両方に登録されているすべてのエンドポイントとインフラストラクチャデバイスも検出されます。

DHCP 対応エンドポイントの IP アドレスが Cisco Unified CM に登録されていない場合、Cisco Prime Collaboration Assurance によってこのエンドポイントを自動検出できない可能性があります。Cisco Unified CM に登録されているすべての Cisco TelePresence システムについても同様です。

Cisco Prime Collaboration リリース 12.1 SP2 以降の場合

TelePresence のエンドポイントの検出（TC/CE）は、HTTPS フィードバックを受信するために、slot2 を専用スロットとして使用します。再検出の際には必ず、Cisco Prime Collaboration Assurance は、その登録解除と登録を再度行う必要があります。エンドポイントが Managed 対象の状態であり、登録されている場合にのみ、TC/CE HTTPS フィードバックを登録します。

自動検出ユーザ インターフェイスを使用して、Unified Communications Manager のパブリッシャが Cisco Prime Collaboration Assurance に追加されると、設定されている ELM または PLM も検出されて管理されます。これは、Cisco Prime Collaboration Assurance に、ELM または PLM のデバイス タイプと、正しい IP アドレス パターンを使用したクレデンシャル プロファイルが含まれている場合にのみ可能です。

Cisco Prime Collaboration リリース 11.5 以降の場合

自動検出は、非 NAT 環境でのみ動作します。NAT 環境で、エンドポイントまたはサブスクライバをシード デバイスと関連付けるには、シード デバイスの再検出を実行し、**[論理検出を有効にする（Enable Logical Discovery）]** ボタンを選択します。

自動検出は、非MSP展開でのみ動作します。MSP展開で、エンドポイント、サブスクライバ、ゲートウェイなどのデバイスをクラスタに関連付けるには、関連付けられているすべてのデバイスを Cisco Prime Collaboration Assurance で管理し、クラスタのパブリッシャ CUCM を再検出する必要があります。

Unified Contact Center デバイスを検出するには、タスクのシード デバイスとして CVP - OAMP サーバを入力する必要があります。

デバイスを自動検出するには、次のようにします。

始める前に

自動検出を実行する前に、次のセクションを確認する必要があります。

- デバイス クレデンシャルの管理：検索を実行する前に、必要なクレデンシャルを入力する必要があります。
- 検出方法：導入に基づいて、適切な導入方法を選択します。
- 前提条件と推奨事項：デバイスに必要な設定を構成し、推奨事項を確認します。
- クラスタのセットアップ：複数の 、Cisco TMS、または CTX クラスタを管理している場合は、特定のアプリケーションの詳細を入力する必要があります。

ステップ 1 選択 **[インベントリ（Inventory）]** > **[インベントリ管理（Inventory Management）]**。

Cisco Prime Collaboration リリース 11.1 以前の場合

移行方法 **[デバイスインベントリ（Device Inventory）]** > **[インベントリ管理（Inventory Management）]**。

ステップ 2 [インベントリの管理（Inventory Management）] ページで、[自動検出（Auto Discovery）] をクリックします。

ステップ 3 ジョブ名を入力して、[デバイスアクセシビリティのチェック（Device Accessibility）] チェックボックスをオンにします。

ステップ 4 検出方法を選択します。使用に最適な検出オプションの詳細については、および前提条件と推奨事項を参照してください。

（注） **Cisco Prime Collaboration リリース 11.5 以降の場合**

[検出（Discover）] ドロップダウンリストから [Communications Manager（UCM）クラスタおよび接続デバイス（Communications Manager (UCM) Cluster and connected devices）]「」 を選択すると、ステップ 7 と 8 で説明されている追加の自動設定オプションが表示されます。

ステップ 5 デバイスの IP アドレスまたはホスト名を入力します。検索プロトコルが単一でない場合は、次のように入力します。

例：

- 論理検出、Cisco Discovery Protocol、および直接検出の場合は、サポートされるデリミタの 1 つ（カンマ、コロン、パイプ、または空白）を使用して複数の IP アドレスまたはホスト名を入力できます。
- **Cisco Prime Collaboration リリース 11.5 以降の場合**

  Communications Manager（UCM）クラスタおよび接続デバイス、Video Communications Server（VCS）/ Expressway クラスタおよび接続デバイス、Telepresence Management Suite（TMS）および接続デバイス、Contact Center Customer Voice Portal（CVP）および接続デバイス、VCenter および接続 ESXi デバイス、UCS Manager 検出、CDP 検出を使用したネットワーク デバイス、直接検出の場合は、サポートされるデリミタの 1 つ（カンマ、コロン、パイプ、または空白）を使用して複数の IP アドレスまたはホスト名を入力できます。

- ping スイープ検出を使用したネットワーク デバイスでは、/netmask 指定を使用し、IP アドレス範囲をカンマで区切って指定します。たとえば、172.20.57.1 から始まり、172.20.57.255 で終わる ping スイープ範囲を指定する場合は、172.20.57.1/24 を使用します。

Cisco Prime Collaboration Assurance を MSP モードで展開した場合は、デバイスを検出するお客様を選択することができます。非 NAT 環境では、パブリック IP（管理 IP）には検出された IP アドレスが入力され、プライベート IP にはデフォルトでパブリック IP（管理 IP）が入力されます。Cisco Prime Collaboration Assurance を Enterprise モードで展開した場合は、デバイスを検出する **Assurance ドメイン** を選択できます。自動検出によって検出されたすべてのエンドポイントは、シード デバイス用に選択された同じ **Assurance ドメイン**に関連付けられます。

Cisco Prime Collaboration リリース 11.5 以降の場合

Cisco Prime Collaboration Assurance を MSP モードで展開した場合は、デバイスを検出するお客様を選択することができます。非 NAT 環境では、パブリック IP（管理 IP）には検出された IP アドレスが入力され、プライベート IP にはデフォルトでパブリック IP（管理 IP）が入力されます。Cisco Prime Collaboration Assurance を Enterprise モードで展開した場合は、検出するデバイスの **ドメインに関連付け**オプションを選択できます。自動検出によって検出されたすべてのエンドポイントは、シード デバイス用に選択された同じ [ドメインに関連付け（Associate to Domain）]に関連付けられます。

ステップ 6 （任意）[Filter] および [Advanced Filter] の詳細を入力します（論理、CDP、および ping スイープ検出方法の場合のみ使用可能）。ワイルドカードを使用して、含めるか、または除外する IP アドレスと DNS 情報を入力することができます。フィールドの説明については、「検出フィルタとスケジュールオプション」を参照してください。

ステップ 7 （任意）ステップ 4 で、[検出（Discover）] ドロップダウンリストから [Communications Manager（UCM）クラスタおよび接続デバイス（Communications Manager (UCM) Cluster and connected devices）]「」を選択し、Unified Communications Manager サーバで CDR 課金サーバの自動設定を有効にしない場合は、[自動設定（Auto-Configuration）] ペインで、[Unified CM サーバで Prime Collaboration サーバを CDR 接続先として追加する（Add the Prime Collaboration Server as a CDR Destination in the Unified CM Servers）] チェックボックスをオフにしてください。

（注） CDR 課金サーバの自動設定の一部として、Cisco Prime Collaboration Assurance は、Unified Communications Manager のパブリッシャとサブスクライバの両方で CDR フラグと CMR フラグを有効にします。ただし、Cisco Prime Collaboration Assurance が CDR 課金サーバの自動設定を実行するのは、管理対象の Unified Communications Manager のパブリッシャのみです。

ステップ 8 （**Cisco Prime Collaboration リリース 11.5 以降の場合**）（任意）ステップ 4 で、[検出（Discover）] ドロップダウンリストから [Communications Manager（UCM）クラスタおよび接続デバイス（Communications Manager (UCM) Cluster and connected devices）] 「」を選択し、Unified Communications Manager サーバで syslog 受信者の自動設定を有効にしない場合は、[自動設定（Auto-Configuration）] ペインで、[Unified CM サーバで Prime Collaboration サーバを syslog 送信先として追加する（Add the Prime Collaboration Server as a CDR Destination in the Unified CM Servers）] チェックボックスをオフにしてください。

（注） Cisco Prime Collaboration Assurance は、syslog 受信者の自動設定を、管理対象の Unified Communications Manager のパブリッシャだけでなく、サブスクライバに対しても実行します。Unified Communications Manager は、設定されたすべての Syslog 受信者に対して、アラームおよびイベントのレベルを「情報」に更新します。

ステップ 9 定期的な検出ジョブをスケジュールするか（フィールドの説明については「検出フィルタとスケジュール オプション」を参照）、またはステップ 10 に従って検出ジョブをすぐに実行します。

ステップ 10 [すぐに実行（Run Now）] をクリックして検出ジョブをすぐに実行するか、[スケジュール（schedule）] をクリックして定期的な検出ジョブをスケジュールし、後で実行します。検索スケジュールを設定している場合は、ジョブの作成後に通知が表示されます。[ジョブの進行状況（Job Progress）] をクリックすると、[ジョブの管理（job management）]ページにジョブのステータスを表示できます。あるいは、すぐに検出を実行している場合は、[デバイス ステータスの概要（Device Status Summary）] ハイパーリンクをクリックして、検出対象のデバイスの現在の状態を確認することができます。

（注）
- Unified Communications Manager の特定のノードを削除すると、Cisco Prime Collaboration Assurance によって、そのノードの IP アドレスの syslog または CDR の設定も削除されます。同じデバイスの、他の syslog または CDR の設定変更は、影響を受けません。
- CDR 課金サーバまたは syslog 受信者の自動設定や手動設定が、Unified Communications Manager のパブリッシャあるいはそのいずれかのサブスクライバで利用できない場合、システムは、デバイスの [ステータス理由（Status Reason）] を [部分管理対象（Partially Managed）]「」 と表示し、同時にその理由（たとえば、「デバイス上の syslog 設定が見つからない」など）も表示します。ただし、Cisco Prime Collaboration Assurance では、デバイスの状態は 「[管理対象（Managed）]」 のままです。

トラブルシューティング

1. **問題**：Cisco Prime Collaboration Assurance がデバイスに CDR アプリケーション課金サーバとして追加されない。

   推奨処置：

   - [自動検出（Auto Discovery）]「」オプションを使用して、Unified Communications Manager のパブリッシャが Cisco Prime Collaboration Assurance に追加されていることを確認します。
   - インベントリを検出した後、デバイスが Managed の状態であることを確認します。また、デバイスは、[コール品質データ ソース（Call Quality Data Source）] の下に表示される必要があります。**[アラームおよびレポート管理（Alarm & Report Administration）] >[CDS ソース設定（CDR Source Settings）]**。
   - [Unified Communications Managerの管理（Unified Communications Manager Administration）] ページで、[サービスアビリティ（Serviceability）]ページを選択し、[CDR管理（CDR Management）] ページに移動します。自動設定が実行されるように、少なくとも 1 台の CDR 課金サーバが使用可能であることを確認してください。

2. **問題**：Cisco Prime Collaboration Assurance がデバイスのリモート Syslog 受信者として追加されない。

   推奨処置：

   - [自動検出（Auto Discovery）]「」オプションを使用して、Unified Communications Manager のパブリッシャが Cisco Prime Collaboration Assurance に追加されていることを確認します。
   - インベントリを検出した後、デバイスが Managed の状態であることを確認します。

- [Unified Communications Manager の管理（Unified Communications Manager Administration）] ページで、[サービスアビリティ（Serviceability）] ページを選択し、**[アラーム（Alarm）]** > **[設定（Configuration）]**。自動設定が実行されるように、少なくとも 1 台の Syslog 受信者が使用可能であることを確認してください。

3. **問題**: TMS 検出では、一部の接続済みデバイスが検出されるわけではありません。

   推奨処置：

   Cisco Prime Collaboration Provisioning Assurance 12.1 以降は、TMS の検出によって、TMS で管理されている CUCM、VCS、およびエンドポイントを自動的に検出しません。

検出フィルタとスケジュール オプション

検出のフィルタ

次の表に、検出の実行の際に使用可能なフィルタを示します。

表 *15* : 検出のフィルタ

フィルタ	説明
[IPアドレス（IP Address）]	included または excluded デバイスのカンマ区切りの IP アドレスまたは IP アドレス範囲。1 ～ 255 のオクテット範囲では、アスタリスク（*）ワイルドカードを使用するか、[xxx-yyy] 表記を使用して制限します。次に例を示します。 • 172.20.57/24 サブネット内にあるすべてのデバイスを含める場合は、172.20.57.* という組み込みフィルタを入力します。 • 172.20.57.224 から 172.20.57.255 の IP アドレス範囲内のデバイスを除外するには、172.20.57.[224-255] の除外フィルタを入力します。 両方のワイルドカード タイプを同じ範囲で使用することができます。例：172.20.[55-57].* 組み込みフィルタと除外フィルタの両方が指定されている場合は、除外フィルタが適用されてから組み込みフィルタが適用されます。自動検出されたデバイスにフィルタを適用すると、その他のフィルタ基準はデバイスに適用されません。デバイスに複数の IP アドレスがある場合、include フィルタを満たす IP アドレスが 1 つの場合に限り、デバイスが自動検出に対して処理されます。
詳細フィルタ	

フィルタ	説明
DNS ドメイン	included または excluded デバイスのコンマ区切りの DNS ドメイン名。 アスタリスク（*）ワイルドカードは、任意の長さ、任意の英数字、ハイフン（-）、およびアンダースコア（_）の組み合わせに一致します。 疑問符（?）のワイルドカードは、単一の英数字、ハイフン（-）、またはアンダースコア（_）に一致します。 たとえば、「*. cisco.com」は、「cisco.com」で終わる任意の DNS 名と一致し、「*.?abc.com」は、「aabc.com」や「babc.com」などで終わる任意の DNS 名と一致します。
Sys Location	（CDP 方式と ping スイープ検出方式でのみ使用できます。）included または excluded デバイスに対する、MIB-II の ysLocation OID に保存されたコンマ区切りの文字列値に一致するコンマ区切りの文字列。 アスタリスク（*）ワイルドカードは、英数字、ハイフン（-）、アンダースコア（_）、および空白文字（スペースとタブ）を任意の長さで組み合わせたものに一致します。たとえば、San * という SysLocation フィルタは、San Francisco、San Jose などで始まるすべての SysLocation 文字列に一致します。 疑問符（?）のワイルドカードは、1 つの英数字、ハイフン（-）、アンダースコア（_）、または空白文字（スペースまたはタブ）と一致します。

Schedule Options

次の表で、使用可能なスケジュール オプションについて説明します。

表 *16 : Schedule Options*

フィールド	説明
Start Time	[開始時刻（Start Time）] をクリックして、開始の日時を yyyy/MM/dd と hh:mm AM/PM の形式で入力します。 カレンダーから開始日と開始時刻を選択する場合は、日付ピッカーをクリックします。表示される時刻は、クライアント ブラウザの時刻です。スケジューリングされた定期的ジョブは、この指定時刻に実行されます。
繰り返し	[なし（None）]、[毎時（Hourly）]、[毎日（Daily）]、[毎週（Weekly）]、[毎月（Monthly）] のいずれかをクリックし、ジョブの期間を指定します。
設定	ジョブ期間の詳細を指定します。
終了時刻	終了日時を指定する必要がない場合は、[終了日時なし（No End Date/Time）] をクリックします。[Every number of Times] をクリックして、指定した期間にジョブが終了するまで、そのジョブが実行される回数を設定します。終了日と終了時刻をそれぞれ yyyy/MM/dd と hh:mm AM/PM 形式で入力します。

デバイスの手動検出

[デバイス ワーク センター（Device Work Center）][デバイス管理（Inventory Management）] ページで [デバイスの追加（Add Device）] オプションを使用して、1 つまたは複数のデバイスを Cisco Prime Collaboration Assurance に手動で追加できます。

新しいデバイスを追加し、検出を実行するには、次の手順を実行します。

始める前に

デバイスを追加する前に、次のセクションを確認する必要があります。

- デバイス クレデンシャルの管理：検索を実行する前に、必要なクレデンシャルを入力する必要があります。
- 検出方法：導入に基づいて、適切な導入方法を選択します。
- 前提条件と推奨事項：デバイスに必要な設定を構成し、推奨事項を確認します。

ステップ 1 選択 **[デバイスインベントリ（Device Inventory）]** > **[インベントリ管理（Inventory Management）]**。

Cisco Prime Collaboration リリース 11.5 以降の場合

移行方法 **[インベントリ（Inventory）]** > **[インベントリ管理（Inventory Management）]**。

ステップ 2 [インベントリ管理（Inventory Management）] ページで、**[デバイスの追加（Add Device）]** をクリックします。

ステップ 3 [デバイスの追加（Add Device）] ウィンドウで、必要な情報を入力します。異なるクレデンシャルの詳細については、[Credential Profiles] のフィールドの説明 を参照してください。

展開に基づいて、[デバイス情報（Device Information）] ペインでデバイスを追加する [顧客（Customer）] または[ドメインに関連付け（Associate to Domain）] を選択できます。

- NAT：検出対象のデバイスが NAT 環境内にある場合は、このチェックボックスをオンにします。
- 顧客：デバイスを検出する顧客を選択できます。
- IP アドレス：パブリック IP アドレスまたは管理対象 IP を入力します。IPv4 アドレスまたは IPv6 アドレスを入力できます。
- プライベート IP アドレス：プライベート IP アドレスを入力します。IPv4 アドレスまたは IPv6 アドレスを入力できます。
- プライベート ホスト名：プライベート ホスト名を入力します。

（注） Cisco Prime Collaboration Assurance を MSP モードで展開した場合は、Unified CM または ELM に登録されているエンドポイントを設定する際に、[プライベートホスト名（Private Host Name）] フィールドに FQDN を入力する必要があります。

（注） 各顧客のデバイスを個別のインスタンスに追加する必要があります。1 つのインスタンスで 1 つの顧客に対して最大 5 台のデバイスを追加できます。デバイスを追加するには、[デバイスの追加（Add Device）] ボタンをクリックします。空の行を必ず削除してください。

ステップ 4 [Discover] をクリックします。検出ジョブのステータスは、[ジョブの管理（Job Management）] ページで確認できます。デバイスは、検出後にインベントリ テーブルに表示されます。詳細については、「検出ステータスの確認」を参照してください。

また、[Assuranceインベントリの概要（Device Status Summary）] を表示して、検出されたデバイスの数と、検出が進行中のデバイスの数を確認することもできます。

ステップ 5 **[検出（Discover）]** をクリックします。ポップアップが表示されます。

Cisco Prime Collaboration リリース 11.5 以降の場合

デバイスの検出が開始されます。検出されるデバイスの現在の状態を確認するには、[デバイスステータスの概要（Device Status Summary）] のハイパーリンクをクリックします。

デバイスのインポート

デバイス リストとクレデンシャルを含むファイルをインポートすることによって、Cisco Prime Collaboration Assurance にデバイスをインポートすることができます。

Cisco Prime Collaboration Assurance を MSP モードで展開した場合は、グローバル カスタマー選択フィールドで選択したお客様のデバイスのみがインポートされます。

デバイスをインポートするには、デバイスごとに次を追加する必要があります。

- ホスト名
- [IP アドレス（IP Address）]
- プロトコルのクレデンシャル

（注） クレデンシャルはプレーンテキストでも暗号化してもかまいませんが、同じファイルに両方を追加することはできません。

- デバイスが NAT 環境にある場合は、そのデバイスの顧客名、プライベート IP アドレスとパブリック IP アドレス、およびプライベート ホスト名を追加してください。
- Cisco Prime Collaboration Assurance を MSP モードで展開した場合は、Unified CM または ELM に登録されているエンドポイントを設定する際に、ホスト名を FQDN として指定する必要があります。
- パブリッシャに登録されているすべてのエンドポイントまたはサブスクライバは、パブリッシャから顧客名を継承します。

（注） デバイスの詳細のみを変更するようにしてください。それ以外の行を変更すると、このファイルが破損し、インポート タスクが失敗する原因になります。

ファイルからデバイスをインポートするには、次のようにします。

始める前に

デバイスをインポートする前に、次のセクションを確認する必要があります。

- デバイス クレデンシャルの管理（Manage Device Credentials）：デバイスの管理に必要なクレデンシャル。
- 検出方法：導入に基づいて、適切な導入方法を選択します。
- 前提条件と推奨事項：デバイスに必要な設定を構成し、推奨事項を確認します。
- デバイスリストとクレデンシャルのエクスポート（Export Device Lists and Credentials）：インポートとエクスポートのファイル形式は同じです。

ステップ 1 選択 **[デバイスインベントリ（Device Inventory）]** > **[インベントリ管理（Inventory Management）]**。

Cisco Prime Collaboration リリース 11.5 以降の場合

移行方法 **[インベントリ（Inventory）]** > **[インベントリ管理（Inventory Management）]**。

ステップ 2 **[インポート（Import）]** をクリックします。

警告 **Cisco Prime Collaboration リリース 11.5 以降の場合**

セキュリティ上の理由により、エクスポートされたデバイスのクレデンシャル ファイルは、同じサーバ上でのみインポートできます。

ステップ 3 [インポート（Import）]ダイアログボックスで、インポートするデバイスとクレデンシャルのリストを含むファイルを参照します。（CSV または XML ファイル形式のみがサポートされています）。暗号化されたクレデンシャルを含むファイルをインポートする場合は、[ファイルは暗号化されたクレデンシャルを含む（File contains Encrypted Credentials）] チェックボックスをオンにします。

ステップ 4 **[インポート（Import）]** をクリックします。

（注） シードまたはパブリッシャ デバイスに対し、インポートベースの検出を実行すると、クラスタ名などの登録済みエンドポイントの登録や関連付けの情報が、完全には取得できません。このような場合は、シードデバイスの再検出を実行して、登録と関連付けの情報を完全に取得してください。

インポートされたデバイスのステータス理由は、デバイスの再検出を実行すると更新されますが、自動検出がそのデバイスを検出するまで待てば更新されます。

インポートされたデバイス リストとクレデンシャルに対するクレデンシャル プロファイルは作成されません。インポート後に、デバイス検出が自動的にトリガーされます。このときに使用されるのは、インポートファイルにあるクレデンシャルです。インポートベースの検出ジョブのステータスは、[ジョブ管理（Job Management）]ページで確認できます。詳細については、「検出ステータスの確認」を参照してください。インポートされたデバイスのクレデンシャルが正しくない場合は、そのデバイスは [Managed] 状態になることができません。

検出後に、インポートされたデバイスがインベントリに表示されます。他のデバイスの詳細、物理情報、アクセス情報は、インベントリ テーブルの下にあるそれぞれのペインに表示されます。また、[デバイス ステータスの概要（Device Status Summary）] を表示して、検出されたデバイスの数と、検出が進行中のデバイスの数を確認することもできます。

デバイス リストとクレデンシャルのエクスポート

デバイス リストとデバイスのクレデンシャルをファイルにエクスポートできます。このファイルを使用して、デバイス リストとクレデンシャルを変更し、後でインポートすることができます。この機能は、ネットワーク管理者、システムの上級管理者、およびシステム管理者の役割を持つユーザのみが使用できます。

デバイス リストとクレデンシャルをエクスポートするには、次の手順を実行します。

ステップ 1 を選択します。**[デバイスインベントリ（Device Inventory）] > [インベントリ管理（Inventory Management）] > [エクスポート（Export）]**。

Cisco Prime Collaboration リリース 11.5 以降の場合

移行方法 **[ベントリ（Inventory）] > [インベントリ管理（Inventory Management）] > [エクスポート（Export）]**

ステップ 2 [デバイス リストとクレデンシャル（Device list and Credentials）] を選択し、出力ファイル名を入力します（サポートされているのは、CSV および XML ファイル形式のみです）。

ステップ 3 [Export] をクリックします。このファイルに含まれているのは、暗号化されたクレデンシャルのみです。

Cisco Prime Collaboration リリース 11.5 以降の場合

警告 セキュリティ上の理由により、エクスポートされたデバイスのクレデンシャル ファイルは、同じサーバ上でのみインポートできます。

ステップ 4 ダイアログボックスが表示されたら、次のいずれかの操作を実行します。

- [開く（Open）] をクリックして情報を確認します。
- [保存（Save）] をクリックして、CSV または XML ファイルをローカルのシステムに保存します。

（注） デバイスが NAT 環境にある場合は、顧客名、プライベート IP アドレスとパブリック IP アドレス、およびプライベート ホスト名も更新されます。

トラブルシューティング

1. **問題**：1 つのサーバから別のサーバにデバイス クレデンシャルをインポートするときに、デバイスが検出されません。

   推奨事項：エクスポートされたデバイス クレデンシャル ファイルは、同じサーバ上のみでインポートできます。

2. **問題**：最新リリースにインポートするため、以前のリリースでエクスポートしたクレデンシャルを使用したときにデバイスが検出されません。

   推奨事項：エクスポートされたデバイス クレデンシャル ファイルは、同じサーバ上のみでインポートできます。

Cisco Unified Computing System（UCS）の検出

次の手順を実行して、NAT 導入環境内の Cisco UCS を検出し、vCenter、ESX、UCS Manager デバイスが Cisco Prime Collaboration Assurance に追加されていることを確認します。

始める前に

- 非 NAT 展開では、VMware vCenter Server（vCenter）、VMware ESX Server（ESX）、および Cisco UCS Manager（UCS Manager）デバイスがサポートされる必要があります。
- 検出中に仮想マシン（VM）の電源をオンにする必要があります。

（注） 新たに追加された仮想マシン（VM）の中で、ポーリングまたは ESXi ホストの再検出によって検出されないものは、論理検出を使用して検出することができます。

- 検出を実行する前に、VMware ツールを VM にインストールする必要があります。これにより、VMware ESX サーバの検出中にツールが確実に検出されます。
- NAT 導入では、管理対象 ESX サーバ内の VM 名は、Cisco Prime Collaboration Assurance 内の VM のプライベート ホスト名と同じである必要があります。
- vCenter を設定し、UCS ブレードでイベントおよびアラームの相関ルールを確認します。詳細については、「vCenter の構成 （165 ページ）」を参照してください。
- Cisco UCS Manager の SNMP を有効にして設定し、SNMP マネージャと SNMP エージェント間の関係を作成します。
  1. Cisco UCS Manager で、[管理（Admin）] タブに移動してタブを展開し、[通信サービス（Communication Services）] タブを選択します。
  2. SNMP ウィンドウのフィールドを設定し、変更を保存します。

ステップ 1 Cisco Prime Collaboration Assurance サーバにログインし、次のページに移動します。**[デバイスインベントリ（Device Inventory）] > [インベントリ管理（Inventory Management）]**。

Cisco Prime Collaboration リリース 11.5 以降の場合

Cisco Prime Collaboration Assurance サーバにログインして、**[インベントリ（Inventory）] > [インベントリ管理（Inventory Management）]** に移動します。

ステップ 2 [クレデンシャルの管理（Manage Credentials）] ボタンをクリックすると、VMware ESX Server（ESX）、Cisco UCS MANAGER（UCS manager）、および VMware vCenter Serve（vCenter）のクレデンシャル プロファイルが作成されます。

（注）
- VMware ESX サーバの SNMP クレデンシャルを設定する必要があります。Cisco Prime Collaboration Assurance のデバイスの設定についての詳細は、次の場所にあるリストを参照してください。
  - Cisco Prime Collaboration Assurance のデバイス設定
  - Cisco Prime Collaboration Assurance のデバイス設定
- VMware ESX Server のクレデンシャル プロファイルの HTTP クレデンシャルは、VMware ESX Server デバイスのクレデンシャルと同じである必要があります。
- クラスタ シナリオでは、Cisco UCS Manager のクレデンシャル プロファイルの HTTP クレデンシャルは、プライマリ ファブリック インターコネクト デバイスのクレデンシャルと同じである必要があります。
- スタンドアロン シナリオでは、Cisco UCS Manager のクレデンシャル プロファイルの HTTP クレデンシャルは、ファブリック インターコネクト デバイスのクレデンシャルと同じである必要があります。
- vCenter クレデンシャル プロファイルの HTTP クレデンシャルは、vCenter デバイス管理者のログイン クレデンシャルと同じである必要があります。
- 仮想マシンは、NAT 展開と非 NAT 展開の両方でサポートされています。

ステップ 3 次の論理検出を実行します。

- [ESX 論理検出（ESX Logical Discovery）]：Esx Server の IP アドレスをシード デバイスとして使用し、そこで実行されているすべての VM を検出します。
- [UCS Manager論理検出（UCS Manager Logical Discovery）]：クラスタ シナリオでは、Cisco UCS Manager の仮想 IP アドレスを、論理検出のシード IP アドレスとして使用します。UCS Manager が管理している UCS シャーシを検出し、さらに、管理対象 ESX サーバを適切な UCS シャーシに関連付けます。スタンドアロン シナリオでは、ファブリック インターコネクト デバイスの IP アドレスを論理検出のシード IP アドレスとして使用します。
- [vCenter 論理検出（vCenter Logical Discovery）]：vCenter IP アドレスをシード デバイスとして使用し、vCenter サーバで管理される vCenter および ESX のサーバを検出します。

（注）
- 管理対象 ESX server 内の VM 名は、VM のプライベート ホスト名と同じであり、Cisco Prime Collaboration Assurance で VM を適切にグループ化できる必要があります。
- 論理検出は MSP 展開ではサポートされていません。

NAT を導入していない環境で、Cisco UCS および 1 つ以上の関連付けられた仮想マシンを検出するには、次の手順を実行します。

1. **Cisco Prime Collaboration リリース 11.1 以前の場合**

   選択 **[インベントリ管理（Inventory Management）]** > **[自動検出（Auto Discovery）][検出方法（Discovery Methods）]** ドロップダウン リストで **[論理検出（Logical Discovery）]** を選択します。

   Cisco Prime Collaboration リリース 11.5 以降の場合

選択 **[Inventory（インベントリ）]** > **[インベントリ管理（Inventory Management）]** > **[自動検出（Auto Discovery）][検出（Discover）]** ドロップダウン リストで **[UCSマネージャ（UCS Manager）]** を選択します。

vCenter IP アドレスをシード デバイスとして、論理検出を実行します。これにより、vCenter と vCenter で管理される ESX サーバや、ESX サーバの関連する仮想マシン、または Cisco Unified Communications（UC）アプリケーションが検出されます。ESX サーバのモデルには、デバイスが C シリーズであるか、または B シリーズであるかが表示されます。

2. **Cisco Prime Collaboration リリース 11.1 以前の場合**

   （オプション）vCenter で構成されない ESX ホストを個別に検出します。[デバイスの追加（Add Device）]（**[インベントリ管理（Inventory Management）]** > **[デバイスの追加（Add Device）]**）または [インポート（Import）] 機能（**[インベントリ管理（Inventory Management）]** > **[インポート（Import）]**）を使用できますが、論理検索を実行して ESX と VM/UC アプリケーション間の関連付けを取得する必要があります。

   Cisco Prime Collaboration リリース 11.5 以降の場合

   （オプション）vCenter で構成されない ESX ホストを個別に検出します。[デバイスの追加（Add Device）]（**[インベントリ管理（Inventory Management）]** > **[デバイスの追加（Add Device）]**）または [インポート（Import）] 機能（**[インベントリ管理（Inventory Management）]** > **[インポート（Import）]**）を使用できますが、論理検索を実行して ESX と VM/UC アプリケーション間の関連付けを取得する必要があります。

3. （オプション）展開内で UCS Manager を使用している場合は、次のように論理検出を実行します。

   - クラスタ シナリオでは、Cisco UCS Manager の仮想 IP アドレスをシード IP アドレスとして使用します。
   - スタンドアロン シナリオでは、ファブリック インターコネクト デバイスの IP アドレスをシード IP アドレスとして使用します。

   これにより UCS シャーシが検出されます。さらに、管理対象 ESX Server を UCS シャーシに関連付けます。UCS Manager の論理検出によってブレードが検出されない場合は、ブレードを個別に検出する必要があります。UCS ホストの検出後に、UCS manager の論理検出を実行してシャーシとブレードの関連付けを構築します。

（注） UCS シャーシの [インベントリ管理（Inventory Management）] には、IP アドレスの代わりに UCS Manager 名と UCS シャーシ名の組み合わせが表示されます。これは、UCS シャーシには IP アドレスがないためです。

検出が成功すると、インフラストラクチャ グループの下にある [デバイス グループ セレクタ（Device Group Selector）] ペイン内のデバイスまたはアプリケーションに関連付けられている Cisco UCS に関連するグループを表示できます。

UCS-B シリーズ ブレード サーバ グループでは、すべての管理対象 Cisco UCS シャーシと、各シャーシの下の管理対象ブレードが一覧表示されます。シャーシの一覧をクリックすると、右側のペインに特定のシャーシの管理対象ブレードのすべての詳細を表示し、シャーシの下のデバイス セレクタ内の管理対象ブレードの IP アドレスを表示できます。管理下のブレード IP アドレスをクリックすると、そのブレードに

関連付けられている管理対象の仮想マシンである Cisco Unified Communications（UC）アプリケーションのリストが右側のペインに表示されます。

UCS-C シリーズのラック サーバ グループでは、すべての管理対象 ESX サーバがノードとして表示されます。ESX サーバの IP アドレスをクリックすると、ESX サーバ 上で実行中のすべての管理対象仮想マシンまたは Cisco Unified Communications（UC）アプリケーションを右側のペインに表示できます。

vCenter の構成

vCenter で SNMP、トリガー、およびアラームを設定するには、次の手順を実行します。

ステップ 1　vCenter の SNMP の設定

a) vSphere を使用して vCenter にログインし、次のページに移動します。 **[管理（Administration）] > [vCenter Serverの設定（vCenter Server Settings）]**
b) SNMP の設定を構成するには、ページの左側にある [SNMP（SNMP）] メニューを選択します。

ステップ 2　vCenter でのトリガーとアラームの設定

a) 仮想マシンを選択して、次のページに移動します。 **[アラーム（Alarms）] > [定義（Definition）]**。
b) vCenter 名をクリックし、アラームを選択して設定項目を設定します。
c) [トリガー（Triggers）] タブに移動し、次のリンクの「「VMware vCenter Server のアラームのトリガー」」セクションの説明に従ってトリガーを選択します。

- Cisco Prime Collaboration Assurance のデバイス設定
- Cisco Prime Collaboration Assurance のデバイス設定

d) [Alert（Alert）]「」 の状態を選択し、[OK（OK）] をクリックします。
e) [アクション（Actions）] をクリックし、「異常なし -> 警告」、「警告 - > エラー」、「エラー -> 警告」、「警告 -> 異常なし」 のすべてのケースで [繰り返し（Repeat）] を選択します。
f) [OK] をクリックします。

Unified CM クラスタ データの検出

Unified CM パブリッシャが Cisco Prime Collaboration Assurance で管理されるように設定したら、クラスタ データ検出を実行して、追加のインベントリ データを収集する必要があります。この検出は、次の情報を収集するために役立ちます。

- Redundancy group、Devicepool、Location、Region、RouteList、RouteGroup、RoutePattern、Partition などを含むクラスタ設定データこれには、電話、ボイスメール エンドポイント、メディア リソース、ゲートウェイ、およびトランクなどのクラスタでプロビジョニングされたエンティティが含まれます。

- Unified CM クラスタに登録されているすべてのエンティティに関する登録情報。これには、デバイス IP、登録ステータス、エンティティが現在登録されている Unified CM サーバ、最新の登録または登録解除のタイムスタンプ、およびステータス理由が含まれます。

  登録情報はコンフィギュレーションファイルを使用して設定できます。この情報は、電話機やゲートウェイなどのエンティティが登録されているクラスタ内のすべてのサブスクライバ ノードから収集されます。

Cisco Prime Collaboration Assurance は、起動時および 1 日に 1 回、Cisco Unified CM からクラスタ設定を収集します。この定期的な検出データ収集は、デフォルトで毎日午前 0 時に実行されます。このデフォルトのスケジュールは変更することができます。

（注）

- 検出されるのは Unified CM に登録されているエンドポイントだけです。Cisco VCS に登録されているエンドポイントは個別に検出されます。
- SIP デバイスは検出されません。
- Cisco Prime Collaboration Assurance は、混合モードの Cisco Unified CM クラスタをサポートしています。CUCM 混合モードについては、Cisco Unified Communications Manager のメンテナンスとオペレーション ガイドを参照してください。
- Cisco Prime Collaboration Assurance 用に設定された CUCM 混合モードでは、Standard CTI Secure Connection アクセス コントロール グループまたはロールを JTAPI アプリケーション ユーザに関連付けないでください。

クラスタ デバイスの検出をスケジュール

始める前に

Unified CM クラスタ検出を実行する前に、次の条件を満たしている必要があります。

- データは、パブリッシャまたは最初のノードから AXL を介して収集されます。そのため、Publisher は適切な HTTP クレデンシャルが入力されている完全な監視状態にあり、AXL Web Service はこの Publisher で実行されている必要があります。
- Unified CM の バージョン 7.x で動作する Cisco RIS Data Collector。
- Cisco SOAP：Unified CM の他のバージョンで動作している CDRonDemand サービス。
- Unified CM Publisher が [Unified CM] セクションまたは Unified CM Administration の [システム サーバ（System Server）] セクションの名前を使用して構成されている場合、この名前は Cisco Prime Collaboration Assurance サーバから DNS を使用して解決可能である必要があります。そうでない場合は、データ収集が続行されるように、この名前のエントリをホストファイル内で設定する必要があります。
- Unified CM で必要な syslogs とプロセスの設定を Cisco Prime Collaboration Assurance で受信可能にするには、[syslog レシーバ（Syslog Receiver）] のセクションの手順を実行する必要

があります。登録情報の変更は、Cisco Unified CM から関連する syslogs を処理することによって更新されます。

Syslog 処理では、Cisco Unified CM クラスタに登録されたエンティティの次のような変更を検出できます。

- 電話、ボイスメールエンドポイント、ゲートウェイなどのエンティティの登録情報の変更。
- クラスタ内でプロビジョニングされる新しい電話が検出され、インベントリが更新されます。

他のデバイスでも、デバイスからの Syslog の設定が必要な場合があります。必要なデバイスの設定の詳細については、次のリンクにある「syslog レシーバの設定」セクションを参照してください。

- Cisco Prime Collaboration Assurance のデバイス設定
- Cisco Prime Collaboration Assurance のデバイス設定

ステップ 1 選択 **[デバイスインベントリ（Device Inventory）]** > **[インベントリ スケジュール（Inventory Schedule）]** > **[クラスタデータ検出のスケジュール（Cluster Data Discovery Schedule）]**。

Cisco Prime Collaboration リリース 11.5 以降の場合

移行方法 **[インベントリ（Inventory）]** > **[インベントリ スケジュール（Inventory Schedule）]** > **[クラスタデータ検出スケジュール（Cluster Data Discovery Schedule）]**。

Cisco Prime Collaboration リリース 12.1 以降の場合

移行方法 **[インベントリ（Inventory）]** > **[クラスタ デバイス検出スケジュール（Cluster Device Discovery Schedule）]**。

ステップ 2 [適用（Apply）] をクリックして後日の検出のスケジュールを設定するか、または [今すぐ実行（Run Now）] をクリックしてクラスタの検出を即座に実行します。

スケジュールされた定期的なデータ収集の前に以下の変更がクラスタ設定で発生していて、これらの変更をすぐに Cisco Prime Collaboration Assurance に反映させる必要がある場合は、[今すぐ実行（Run Now）] オプションを使用して、次のタイプのデータを収集する必要があり ます。

- クラスタ内で追加、削除、または変更された新しいデバイス プール、Location、Region、Redundancy Group、Route List、Route Group、Route Pattern、または Partition。
- デバイス プールへの任意のエンドポイントのメンバーシップの変更、または任意のエンドポイントの冗長グループへの関連付けの変更。
- Unified CM クラスタに追加された、または Unified CM クラスタから削除された新しいサブスクライバ。
- 冗長グループに対する任意のサブスクライバのメンバーシップでの変更。

- ルート グループへの任意のゲートウェイのメンバーシップ、またはルート リストへのルート グループのメンバーシップの変更。

変更が特定のクラスタに制限されている場合は、次の手順でクラスタのパブリッシャを再検出することができます。**[デバイスインベントリ（Device Inventory）]**>**[インベントリ管理（Inventory Management）]**>**[再検出（Rediscover）]**。

Cisco Prime Collaboration リリース 11.5 以降の場合

変更が特定のクラスタに制限されている場合は、次の手順でクラスタのパブリッシャを再検出することができます。**[デバイスインベントリ（Device Inventory）]**>**[インベントリ管理（Inventory Management）]**>**[再検出（Rediscover）]**。

新しい Unified CM クラスタの場合、検出または再検出の後、そのクラスタの電話機検出が実行されます。他の電話機同期の処理（クラスタの電話機検出、XML の検出など）が進行中の場合、クラスタベースの電話機検出は処理が完了するまで待機します。したがって、他の電話機同期の処理が進行中のときは、Cisco Prime Collaboration Assurance の電話機の状態変更が反映されるまで予想外に時間がかかります。

関連トピック

Cisco Prime Collaboration Assurance のデバイス設定

デバイスの再検出

すでに検出されたデバイスを再検出できます。すでに入力されているクレデンシャルは、Cisco Prime Collaboration Assurance データベースですでに使用可能になっており、変更によってシステムが更新されます。どの状態のデバイスでも再検出できます。

Cisco Prime Collaboration リリース 12.1 SP2 以降の場合

（注） 再検出の際には必ず、Cisco Prime Collaboration Assurance は、登録解除と再登録を行う必要があります。

再検出を実行するのは、次のときです。

- デバイスを最初に追加してから再検出する必要があります。
- ファースト ホップ ルータ設定に変更があり、ソフトウェア イメージを更新するため。
- クレデンシャル、ロケーション、タイムゾーン、IP アドレスやホスト名、SIP URI、H.323 ゲートキーパーのアドレスなどのデバイスの設定が変更されたとき。
- Cisco Prime Collaboration Assurance のバックアップや復元を実行した後。

[現在のインベントリ（Current Inventory）] ペインの [再検出（Rediscover）] ボタンを使用して、[現在のインベントリ（Current Inventory）] テーブルに表示されているデバイスを再検出します。再検出は、単一のデバイスだけでなく、複数のデバイスに対しても実行できます。

[インベントリ管理（Inventory Management）] で以前に管理された IP アドレスを使用して、到達不能になったデバイス（ルータ、スイッチ、または音声ゲートウェイ）の再検出を実行すると、デバイスは、いずれかのインターフェイスの IP アドレスで再検出されます。この動作を変更するには、*emsam.properties* ファイルの *com.cisco.nm.emms.discovery.ip.swap* プロパティの値を**false**に設定します。この場合、デバイス（ルータ、スイッチ、または音声ゲートウェイ）は、インターフェイスの IP アドレスによって再度検出されることはありません。 ここでは、以前に管理された IP アドレスを使用してデバイスを再検出します（[操作（Operate）] > [デバイス ワーク センター（Device Work Center）]）。

Cisco Prime Collaboration リリース 11.1 以前の場合

選択 **[インベントリ管理（Inventory Management）]** を選択して、以前に管理された IP アドレスでデバイスを再検出します。

Cisco Prime Collaboration リリース 11.5 以降の場合

選択 **[インベントリ管理（Inventory Management）]** を選択して、以前に管理された IP アドレスでデバイスを再検出します。

（注） アクセシビリティ情報は、再検出中にはチェックされません。

再検出のワークフローは、検出の場合と同じです。詳細については、「ライフ サイクルの検出」を参照してください。

検出ステータスの確認

すべての検出ジョブのステータスが [ジョブ管理（Job Management）] ページに表示されます。検出を実行すると、[ジョブ進行状況の詳細（Job Progress Details）] リンクを含むダイアログボックスが表示され、検出ステータスを確認できるようになります。検出ジョブの完了までの時間は、ネットワークによって異なります。検出が完了すると、詳細が [現在のインベントリ（Current Inventory）] テーブルに表示されます。

検出ステータスを確認するには、以下を行います。

ステップ 1 Choose を選択します。**[Device Inventory（デバイスインベントリ）] > [インベントリ管理（Inventory Management）] > [検出ジョブ（Auto Jobs）]**。

Cisco Prime Collaboration リリース 11.5 以降の場合

移行方法 **[Inventory（インベントリ）] > [インベントリ管理（Inventory Management）] > [検出ジョブ（Auto Jobs）]**。

ステップ 2 [ジョブ管理（Job Management）] ページで、詳細を表示する検出ジョブを選択します。

検出のステータス、および検出中に検出されたすべてのデバイスが [Job Management] テーブルの下のペインに表示されます。

ステップ 3 [ジョブ管理（Job Management）] テーブルで検出ステータスを確認するか、[ジョブの詳細（Job details）] ペインで検出されたデバイスの詳細を確認します。

ステップ 4 結果に応じて、次のいずれかを実行します。

- 誤ったクレデンシャルが原因で検出されなかったデバイスについては、それらのデバイスのクレデンシャルを確認し、検出を再実行します。
- 同じデバイスを複数回検出するには、Rediscover オプションを使用します。詳細については、「デバイスの再検出」を参照してください。

トラブルシューティング

1. **問題**：Cisco TelePresence Video Communication Server（Cisco VCS）Edgeで、外部インターフェイスの IP アドレスにアクセスできず、アラームが発生する。

   推奨処置：Cisco Unified Communications Manager を検出する前に、Cisco VCS Core および Cisco VCS Edge を検出する必要があります。これにより、Cisco VCS - Edge の外部インターフェイスと内部インターフェイスのすべての IP アドレスが、Cisco Prime Collaboration Assurance インベントリで認識されるようになります。Cisco Unified Communications Manager のパブリッシャが検出されると、インターフェイス IP アドレスは、収集されたインベントリと照合されるため、アクセスできないというアラームが発生しません。

2. **問題**：Cisco TelePresence Management Suite（TMS）に関連付けられたデバイスが検出されない。

   推奨処置：関連付けられたデバイスを検出するように、Cisco TelePresence Management Suite（TMS）の論理検出を実行したことを確認します。[デバイスの追加（Add Device）] オプションは、TMS のみを検出し、関連付けられたデバイスを検出しません。

   [論理検出の有効化（Enable Logical discovery）] オプションを選択して、TMS を再検出します。関連付けられたすべてのデバイスに対して、クレデンシャルが追加されていることを確認します。

3. **問題**：Cisco TelePresence のタッチ パネルで、コーデック エンドポイントに直接接続せずに syslog イベントを送信できない。

   推奨処置：Cisco TelePresence のタッチ パネルがコーデックに接続されていて、そのコーデックが Cisco Prime Collaboration Assurance で再検出されることを確認します。

4. **問題**：DX80 や電話機が正常に検出されない。

   推奨処置：DX80 およびその他の電話機は、電話機の同期、CDT、または Cisco Unified Communications Manager のパブリッシャ クラスタ検出の一部としてのみ検出されます。登録や登録解除のステータスとは別に、電話機の任意の設定変更は、クラスタ データ検出の後にのみ、Cisco Prime Collaboration Assurance のインベントリに反映されます。

DX IP アドレスを追加することによって、DX80 デバイスを個別に検出しないでください。

5. **Cisco Prime Collaboration リリース 11.6 以降の場合**

   問題：CE イメージを含む CiscoDX80/DX70 デバイスが正常に検出されない。

   推奨処置：CiscoDX80/DX70 デバイスが Cisco Unified Communications Manager に存在することを確認してください。

   詳細については、『Cisco Prime Collaboration Assurance のデバイス設定』を参照してください。

6. **Cisco Prime Collaboration リリース 11.6 以降の場合**

   問題：CE イメージを含む CiscoDX80/DX70 デバイスが正常に検出され、そのデバイスがアクセス不能な状態になっている。

   推奨処置：CiscoDX80/DX70 デバイスのクレデンシャルプロファイルを追加し、さらに、Cisco Prime Collaboration Assurance が Device360 ビューの ping オプションで、デバイスに ping を実行できることを確認します。

   詳細については、『Cisco Prime Collaboration Assurance のデバイス設定』を参照してください。

7. **Cisco Prime Collaboration リリース 11.6 以降の場合**

   問題：CE イメージを含む CiscoDX80/DX70 デバイスが、サポートされていない状態になっている。

   推奨処置：Ensure Cisco Prime Collaboration Assurance が 11.6 よりも上位のバージョンであることを確認してください。バージョン 11.6 未満の場合は、CE イメージを含む CiscoDX80/DX70 デバイスはサポートされません。

   詳細については、『Cisco Prime Collaboration Assurance のデバイス設定』を参照してください。

8. **Cisco Prime Collaboration リリース 11.6 以降の場合**

   問題：CE イメージを含む CiscoDX80/DX70 デバイスが [会議診断（Conference Diagnostics）] ページに表示されない。

   推奨処置：これらの電話機が登録されている管理対象 Unified CM に対して、適切な JTAPI クレデンシャルが追加されていることを確認してください。

   詳細については、『Cisco Prime Collaboration Assurance のデバイス設定』を参照してください。

9. **問題**：電話機のシリアル番号が見つからない。

   推奨処置：電話機の [デバイス360度ビュー（Device 360° View）] に、シリアル番号が表示されます。デバイス上で**[インベントリ（Inventory）]**>**[インベントリ管理（Inventory Management）]**をクリックして、電話機の IP アドレス上のアイコンをクリックして、[デバイス 360° 表示（Device 360° View）] を起動します。

10. **問題**：Cisco Unified Communications Manager が非 Cisco デバイスとして表示される。

    推奨アクション：Cisco Unified Communications Manager の Cisco Unified Communications Manager SNMP サービスを有効にします。Cisco Prime Collaboration Assurance のデバイスの設定についての詳細は、次の場所にあるリストを参照してください。

    - Cisco Prime Collaboration Assurance のデバイス設定
    - Cisco Prime Collaboration Assurance のデバイス設定

11. **問題**：Cisco Prime Collaboration Assurance のインベントリで、エンドポイント名がすぐに更新されない。

    推奨処置：次のことを確認してください。

    - クラスタに属するエンドポイントのエンドポイント名が更新されるのは、クラスタデータ検出を実行した後のみです。
    - エンドポイントの説明を変更した後、Cisco Unified Communications Manager でエンドポイントをリセットします。エンドポイント名は syslog 通知によって、Cisco Prime Collaboration Assurance ですぐに更新されます。syslog が Cisco Prime Collaboration Assurance で設定されているか確認してください。

12. **問題**：Cisco SocialMiner デバイスにカウンタが読み込まれず、カスタム ダッシュボードに「**使用可能なデータがありません**」と表示される。

    推奨処置：次の条件が満たされていることを確認します。

    - Cisco SocialMiner デバイスが稼働中であり、[インベントリの管理（Inventory Management）] ページに [Managed（Managed）] の状態で表示されることを確認します。
    - ブラウザで次の URL を入力して、サービスが実行されていることを確認します。

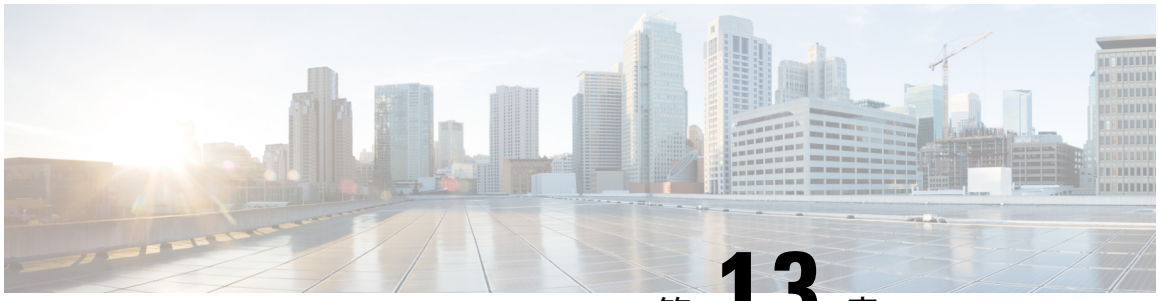
      ```
      http://<ServerIP>:8080/sm-dp/rest/DiagnosticPortal/GetPerformanceInformation
      ```

13. **問題**：CCisco Finesse デバイスにカウンタが読み込まれず、カスタム ダッシュボードに「**使用可能なデータがありません**」と表示される。

    推奨処置：次の条件が満たされていることを確認します。

    - Cisco Finesse デバイスが稼働中であり、[インベントリの管理（Inventory Management）] ページに [管理対象（Managed）] の状態で表示されることを確認します。
    - ブラウザで次の URL を入力して、サービスが実行されていることを確認します。

      ```
      https://<server>/finesse-dp/rest/DiagnosticPortal/GetPerformanceInformation
      ```



第 13 章

デバイス グループの管理

このセクションでは、次の点について説明します。

- デバイス グループの管理 （173 ページ）

デバイス グループの管理

この章では、デバイス グループの管理について説明します。

デバイス グループについて

デバイス グループは自動的に作成されます。デバイス検出後、デバイス グループを、状態に関係なくデバイス タイプに基づいて検索できます。ネットワークに導入し、ライセンスを供与したデバイスのみがグループに表示されます。[デバイス グループ（Device Group）] ペインには、空のグループやデバイスがないグループは表示されません。

デバイスをグループ化すると、単一のデバイス、またはデバイスのグループのデータを表示できるようになります。カスタマイズされたグループを作成して、目的の情報を監視することができます。グループ構造は、[デバイス グループ（Device Group）] ペインで一覧またはツリービューとして表示できます。[デバイス グループ（Device Group）] ペインは、、会議 の診断（Session Conference Diagnostice）]（フィルタとして）、[エンドポイントの診断（Endpoint Diagnostics）]、[アラームとイベント（Alarms and Events）] ページで使用できます。目的のグループからのデバイスまたはエンドポイントを選択、インベントリの詳細を確認、、。[ポーリング パラメータ（Polling Parameters）] ページの [デバイス グループ セレクタ（Device Group Selector）] からは、ポーリングするデバイスを選択することもできます。詳細については、デバイス グループ セレクタを参照してください。

Cisco Prime Collaboration Assurance は、階層形式でグループをサポートしています。それぞれの子グループは親グループのサブグループであり、そのグループ メンバーシップは直接の親グループのサブセットになります。オブジェクトがグループに属するためには、オブジェクトがそのグループのルールと親グループのルールに従っている必要があります。

グループ セレクタ（ツリービュー）が使用可能なページには、手動でグループを作成することもできます。

グループ化は、次のものをフィルタリングするために使用します。

- [インベントリ管理（Inventory Management）] ページのデバイス
- レポート（Reports）
- [会議の診断（Conference Diagnostics）] ページの会議
- [エンドポイントの診断（Endpoint Diagnostics）] ページのエンドポイント
- アラームおよびイベント ブラウザ ページのアラームとイベント
- ランディング ページのダッシュレット

Cisco Prime Collaboration Assurance 内のデバイスは、次のとおりにグループ分けされます。

- システム定義グループ：デバイス タイプに基づき、システムによって定義されています。システム定義グループは常にダイナミックであり、削除または編集できません。

  定義済みグループ：エンドポイント グループに基づき、システムによって定義されています。定義済みグループは常にダイナミックであり、削除または編集できません。使用可能な定義済みグループは、次のとおりです。

  - 音声 IP 電話
  - デスクトップ ビデオ
  - イマーシブ テレプレゼンス
  - IP 電話
  - モバイル エンドポイント
  - 多目的テレプレゼンス
  - パーソナル コミュニケータ
  - パーソナル テレプレゼンス
  - ソフト クライアント
  - TelePresence エンドポイント
  - 不明

    各グループに属するデバイスを確認するには、そのグループのクイック ビュー アイコンの上にマウスを置き、[ルール（Rules）] をクリックします。

- ユーザ定義グループ：次のいずれかになります。

  - スタティック：デバイスは、定義された一連のルールを使用せずに、これらのグループに追加されます。グループが作成された後に、手動でデバイスを追加できます。ルールを簡単に設定できないデバイスは、このグループに入ります。スタティック ユーザ定義グループだけが、[Device Group] から [Polling Parameters] ページの [Device

Selector] ペインに同期されます。ダイナミック グループ内に作成されたスタティック グループも同期化されません。

- ダイナミック：デバイスは、定義した一連のルールまたは属性（たとえば、デバイス タイプ、デバイス モデル、ホスト名など）に基づき、グループへのアクセス時に ダイナミック グループに追加されます。グループのプロパティを使用してルールを定義することができ、グループはルールが適用されたときに更新されます。

（注） ユーザ定義のダイナミック グループの作成にかかる時間は、グループ内のメンバー数によって異なります。

ユーザ定義のダイナミックおよびスタティック グループの場合は、クイックビューを使用してサブグループを追加、ならびグループを編集、削除、複製することができます。ダイナミック グループの場合、ダイナミック サブグループを作成または追加すると、親のグループのルールを自動的に継承します。

クイック ビューを起動するには、マウス ポインタをデバイス グループの上に置き、[クイック ビュー（Quick View）] アイコンをクリックします。クイック ビューに表示されるユーザ定義グループの詳細は、次のとおりです。

表 *17*：ユーザ定義グループ用のクイック ビューの詳細

フィールド	説明
Name	デバイスの名前。
説明	デバイスの説明。
タイプ	デバイスのタイプです。
グループ タイプ	グループ タイプ（ダイナミックまたはスタティック）を表示します。
メンバー数	グループ内のメンバーの合計数が表示されます。
サブグループ数	グループ内のサブグループ数を表示します。グループには任意の数のサブグループを追加できます。
ルール数	グループに設定されているルールの数を表示します。 （注） ルールの詳細を確認するには、[Number of Rules] の上にマウスを移動し、クイック ビュー アイコンをクリックします。

フィールド	説明
サブグループの追加	1. [Add SubGroup] をクリックします。 2. [Create SubGroup] ウィンドウで、サブグループの詳細を入力します。 3. [保存（Save）] をクリックします。 ダイナミック グループ内にスタティック グループを作成することも、その逆もできます。スタティック サブグループを作成した場合、親のダイナミック グループのルールは継承されません。スタティック サブグループは、任意の階層で作成された個別のグループです。 ダイナミック グループの場合、ダイナミック サブグループを作成すると、親のグループのルールを自動的に継承します。
グループの編集	1. [Edit Group] をクリックします。 2. [Edit Group] ウィンドウで、必須フィールドを編集します。 3. [保存（Save）] をクリックします。 グループ名と説明を編集し、親グループを選択することができます。
グループの削除	1. [Delete Group] ボタンをクリックします。 2. 確認メッセージボックスで [OK] をクリックします。
グループの複製	1. [Duplicate Group] をクリックします。 2. [Duplicate Group] ウィンドウで、グループの詳細を入力します。 3. [保存（Save）] をクリックします。 ダイナミック グループで [グループの複製（Duplicate Group）] を実行すると、ルールのプロパティは新しいグループにコピーされます。

グループの作成

グループを作成するには、次の手順を実行します。

ステップ 1 [デバイスグループ（Device Group）] ペインの右にあるアイコンをクリックします。

ステップ 2 [Create Group] をクリックします。

ステップ 3 [Create Group] ウィンドウで、グループ名と説明を入力します。

ステップ 4 [スタティック（Static）] または [ダイナミック（Dynamic）] のグループ タイプを選択します。

ステップ 5 ダイナミック グループの場合は、[すべて一致（Match as All）] または [任意の条件（Match as Any）] を選択してルールを設定し、ドロップダウン リストから適切な条件の組み合わせを選択します。

[+] をクリックすると複数のルールを設定できます。新しい行が追加されます。

ステップ 6 [保存（Save）] をクリックします。

グループにデバイスを追加

デバイスをグループに追加するには、次のようにします。

ステップ 1 を選択します。**[デバイスインベントリ（Device Inventory）]** > **[インベントリ管理（Inventory Management）]**。

Cisco Prime Collaboration リリース 11.5 以降の場合

移行方法 **[インベントリ（Inventory）]** > **[インベントリ管理（Inventory Management）]**

ステップ 2 [Current Inventory] テーブルから管理対象デバイスを選択します。

ステップ 3 [Current Inventory] ペインで右矢印をクリックします。

ステップ 4 [グループに追加（Add to Group）] を選択します。

ステップ 5 [グループに追加（Add To Group）] ウィンドウで、[グループの選択（Select Group）] ドロップダウンリストから目的のグループを選択し、[保存（Save）] をクリックします。

（注） デバイスの追加や削除ができるのは、ユーザ定義のスタティック グループだけです。ユーザ定義のダイナミック グループにデバイスを追加することはできません。

グループからデバイスを削除

デバイスを削除するには、次の手順を実行します。

ステップ 1 を選択します。**[デバイスインベントリ（Device Inventory）]** > **[インベントリ管理（Inventory Management）]**。

Cisco Prime Collaboration リリース 11.5 以降の場合

移行方法 **[インベントリ（Inventory）]** > **[インベントリ管理（Inventory Management）]**

ステップ 2 **インベントリ管理** ページで、[現在のインベントリ（Current Inventory）] テーブルから管理対象デバイスを選択します。

ステップ 3 [Current Inventory] ペインで右矢印をクリックします。

ステップ 4 [グループから削除（Remove From Group）] を選択します。

ステップ 5 確認メッセージ ボックスで [OK] をクリックします。

デバイス グループ セレクタ

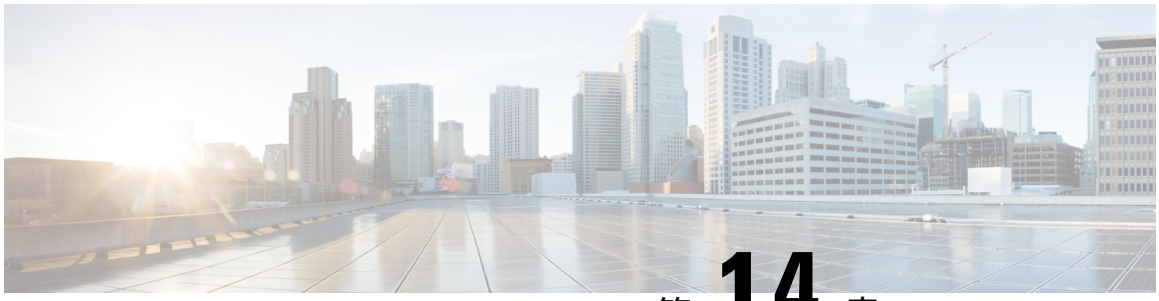
デバイス グループ セレクタはデバイスをフィルタ処理する方法で、[ポーリング パラメータ（Polling Parameters）] ページを開くには、を選択します。**[アシュアランス管理（Assurance Administration）]** > **[ポーリング設定（Polling Settings）]**を選択し、ポーリングするグループを選択します。

Cisco Prime Collaboration リリース 11.5 以降の場合

選択 **[アラームおよびレポート管理（Alarm & Report Administration）]** > **[ポーリング設定（Polling Settings）]** を選択し、ポーリングするグループを選択します。

関連トピック

ポーリングの設定 （237 ページ）



第 14 章

インベントリの管理

このセクションでは、次の点について説明します。

- インベントリの管理 （179 ページ）
- インベントリ詳細の表示 （179 ページ）
- デバイス固有のインベントリ詳細 （202 ページ）
- インベントリ詳細の更新と収集 （218 ページ）
- 管理対象デバイスの一時停止と再開 （223 ページ）
- デバイスの削除 （224 ページ）
- パフォーマンス グラフ （226 ページ）
- Unified CM デバイスの検索 （233 ページ）
- SNMP クエリ（SNMP Query） （235 ページ）

インベントリの管理

この章では、インベントリの管理について説明します。

インベントリ詳細の表示

Cisco Prime Collaboration Assurance は、リアルタイムによる検出を継続して行います。ネットワークに関する最新情報を取得するには、定期的にインベントリを更新する必要があります。インベントリをどの程度の頻度で更新するかをスケジュールできます。

インベントリを更新すると、インベントリは Cisco Prime Collaboration Assurance データベースと同期されます。Cisco Prime Collaboration Assurance は、更新後にネットワークで発生したすべての追加、削除、変更を反映させます。

Cisco Prime Collaboration Assurance では、デバイスはデバイス タイプに基づきグループ化されます。[デバイス グループ（Device Group）] ペインは、[インベントリ管理（Inventory Management）]、会議の診断（Session Conference Diagnostice）]（フィルタとして）、[エンドポイントの診断（Endpoint Diagnostics）]、[アラームとイベント（Alarms and Events）] ページで

使用できます。対象のグループからデバイスまたはエンドポイントを選択し、インベントリの詳細を確認を監視できます。

（注） Cisco Prime Collaboration Assurance で TC/CE デバイス タイプとして検出された Cisco Telepresence エンドポイントは、JTAPI ユーザーが制御するデバイス リストには含めないようにします。IP フォンは、JTAPI ユーザの制御リストで保持することを推奨します。

インベントリ テーブルのデバイス ホスト名列にマウスを乗せて [デバイス 360°（Device 360°）] ビューをクリックすると、アラーム、インターフェイス、ポート、環境、モジュール、デバイス固有のその他の機能など、デバイスの詳細を確認できます。詳細については、デバイスの 360° ビューを参照してください。インベントリ テーブルには、Unified Communications Manager に登録され、管理対象であるデバイスのソフトウェア バージョンも表示されます。デバイスには、ソフト フォン、ハード フォン、Jabber があります。

およびインベントリ管理ページには、インベントリ テーブルの他にも、ここの下には、システム情報、アクセス情報、インターフェイス情報、イベント設定ペインが表示されます。すべてのペインは、最後にポーリングされたデータに基づき設定されます。これらのデバイスの詳細を表示するには、少なくとも 1 回は [Managed] 状態となっている必要があります。

インベントリ ペイン

現在のインベントリ テーブルは、 [インベントリ（Inventory）] ページで利用できます。

Cisco Prime Collaboration Assurance により管理される各デバイスは、デバイス（インターフェイスおよび周辺機器）の物理インベントリを表示できるようになっています。デバイスのインベントリ詳細を表示するには、[Current Inventory] ペインの行をクリックします。

複数のデバイス（最初の 500 個の項目）を選択するには、[Current Inventory] ペインの左上隅にあるチェックボックスを使用します。

Cisco Prime Collaboration Assurance を MSP モードで展開した場合、デバイスを選択してデバイスを割り当ててから、[編集（Edit）]>[割り当て（Assign）] をクリックして顧客を割り当てることができます。[デバイスの編集（Edit Device）] ダイアログボックスが表示されたら、ドロップダウンリストから顧客名を選択できます。[デバイス グループ（Device Group）] ペインから、[ホスト名（Recycle Host）] を選択した後（これによりクラスタのすべてのデバイスが選択される）、[編集（Edit）]>[割り当て（Assign）] をクリックすることにより、クラスタに顧客を割り当てることができます。同様に、顧客の割り当てを解除するには、デバイスを選択してから、[編集（Edit）] > [割り当て解除（Unassign）] をクリックします。

[クレデンシャルの変更（Modify Credentials）] オプションを使用して、クレデンシャルと再検出デバイスを変更できます。確認メッセージ ウィンドウで [ジョブの進行状況（Job Progress）] をクリックすると、[ジョブ管理（Job Management）] ページを相互起動して、検出ジョブの詳細を確認できます。

Cisco Prime Collaboration リリース 11.1 以前の場合

[しきい値設定（Threshold Settings）] オプションを使用して、自動トラブルシューティングの有効化、無効化、または設定を切り替えることができます。

[一時停止（Suspend）] オプションや [再開（Resume）] オプションを使用して、デバイスの管理の一時停止や再開ができます。インベントリは、[Suspended] 状態のデバイスについては更新されません。

インベントリ テーブルの [Show] ドロップダウン リストを使用して、デバイス タイプと状態に基づいてデバイスをフィルタリングできます。たとえば、ネットワーク内の、すべての削除されたデバイスを再検出する場合は、表示ドロップダウン リストから [Deleted] を選択します。インベントリ テーブルに、すべての削除されたデバイスの一覧が表示されます。これらのデバイスを検出するために再検出を実行します。

たとえば、ネットワーク内の、すべての削除されたデバイスを再検出する場合は、表示ドロップダウン リストから [Deleted] を選択します。インベントリ テーブルに、すべての削除されたデバイスの一覧が表示されます。これらのデバイスを検出するために再検出を実行します。

クイック フィルタや拡張フィルタなどのオプションがあり、デバイスの条件に基づいてデバイスをフィルタリングできます。

インベントリ テーブルの右上隅にある [Total] フィールドには、デバイス数が表示されます。グループ内のデバイス数を表示するには、グループを選択します。

たとえば、電話機エンドポイントの数を表示するには、[Device Group] で [Endpoints] グループを選択します。[Total] フィールドのエンドポイント数が更新されます。デバイス カウントの詳細については、現在のインベントリ テーブルのフィールド説明欄を参照してください。

不明なエンドポイントの一覧を表示するには、[デバイス グループ セレクタ（Device Group Selector）] > [定義済み（Predefined）] > [不明なエンドポイント（Unknown Endpoints）] の順に選択します。

Cisco Prime Collaboration リリース 12.1 以降の場合

[しきい値設定（Threshold Settings）] オプションを使用して、自動トラブルシューティングの有効化、無効化、または設定を切り替えることができます。

[一時停止（Suspend）] オプションや [再開（Resume）] オプションを使用して、デバイスの管理の一時停止や再開ができます。インベントリは、[Suspended] 状態のデバイスについては更新されません。

インベントリ テーブルの [Show] ドロップダウン リストを使用して、デバイス タイプと状態に基づいてデバイスをフィルタリングできます。

クイック フィルタや拡張フィルタなどのオプションがあり、デバイスの条件に基づいてデバイスをフィルタリングできます。

インベントリ テーブルの右上隅にある [Total] フィールドには、デバイス数が表示されます。グループ内のデバイス数を表示するには、グループを選択します。

たとえば、電話機エンドポイントの数を表示するには、[Device Group] で [Endpoints] グループを選択します。[Total] フィールドのエンドポイント数が更新されます。デバイス カウントの詳細については、「現在のインベントリ テーブルのフィールド説明」テーブルを参照してください。

不明なエンドポイントの一覧を表示するには、**[デバイス グループ セレクタ（Device Group Selector）] > [定義済み（Predefined）] > [不明なエンドポイント（Unknown Endpoints）]** の順に選択します。

この表は、インベントリ テーブルのフィールドについて説明しています。デフォルトでは、インベントリ テーブルのすべての列は表示されません。すべての列を表示するには、右上の隅にある [Settings] オプションをクリックします。CSV または PDF ファイルとして インベントリ テーブルをエクスポートするには、インベントリ テーブルの右上の隅にある [Export] アイコンをクリックします。

表 *18 : [Current Inventory]* テーブルのフィールドの説明

フィールド	説明
エンドポイント名	識別を容易にするためにエンドポイントに割り当てられた名前。
内線番号	エンドポイントのディレクトリ番号です。この数は、デバイスの一意的な識別に役立ちます。
電話の説明	Cisco Unified Communications Manager（CUCM）または Cisco TelePresence Video Communication Server（VCS）でデバイスの設定時に追加した、エンドポイントの特徴を表す説明です。
ホスト名	識別を簡単にするためにデバイスに割り当てられる名前。
モデル	Catalyst3506G48PS などのデバイス モデル。

フィールド	説明
IP Address	デバイスを管理するために使用される IP アドレス。 IP アドレスをクリックすると、そのデバイスにログインできます。 この機能は、MSPモードでは使用できません。 クイック ビューアイコンをクリックして、そのデバイスの デバイス 360 度ビューを起動します。 そのデバイスがエンドポイントの場合、エンドポイントの 360 度ビューが表示されます。 これらのデバイスが論理検出で検出された場合、IP アドレスとプライベート IP アドレスは同じになります。 ルータとスイッチの場合、デバイスにログインするには、Putty などのターミナル クライアント アプリケーションを関連付ける必要があります。
Mac アドレス	デバイスの MAC アドレスです。
[ソフトウェア タイプ（Software Type）]	デバイスで実行している IOS や CentOS などのソフトウェアです。
ソフトウェア バージョン	デバイスで実行しているソフトウェアのバージョンです。 （注） デバイスが Unified Communications Manager に登録されていない場合、[ソフトウェア バージョン（Software Version）] フィールドには NA」と表示されます。
デバイス プール	CUCM に登録されているデバイスのみに使用します。
パーティション	CUCM に登録されているエンドポイントのみに使用します。
シリアル番号	エンドポイントのみに適用されます。
状態	デバイスのステータスです。
ステータス理由	デバイスのステータス理由です。

フィールド	説明
タイプ	デバイスの最適なロールまたはサービスです。
機能	デバイスの他のすべてのロールまたはサービスです。
最終検出日	デバイスが最後に検出された日時です。時刻は、Cisco Prime Collaboration Assurance サーバで設定されているタイムゾーンに従います。
Cisco Prime Collaboration リリース 11.1 以前の場合 カスタマイズされたイベント	• 緑のチェックマークが表示—[イベントのカスタマイズ（Customize Events）] タブを使用して、デバイスのイベント設定がカスタマイズされています。 • 緑のチェックマークが非表示—そのデバイスのイベント設定はカスタマイズされていません。このデバイスはグローバル設定を使用します。
Cisco Prime Collaboration リリース 11.1 以前の場合 Mediatrace Role	• [Unsupported]：デバイスは Cisco Mediatrace をサポートしません。 • [Transparent]：デバイスは Cisco Mediatrace をサポートしますが、プロファイルが設定されていません。 • [Responder]：Cisco Mediatrace の応答側プロファイルがデバイスでイネーブルにされています。Cisco Mediatrace の情報を監視および収集する場合は、このプロファイルを有効にします。 • [Responder]：Cisco Mediatrace の発信側プロファイルがデバイス上でイネーブルにされています。Cisco Mediatrace セッションまたはポーリングを開始する場合は、このプロファイルを有効にします。 • [Initiator/Responder]：Cisco Mediatrace の発信側および応答側プロファイルがデバイスでイネーブルにされています。

フィールド	説明
Cisco Prime Collaboration リリース 11.1 以前の場合 IP SLA Role	• 非対応—デバイスはビデオ IP SLA をサポートしていません。 • 未設定—デバイスはビデオ IP SLA をサポートしますが、設定されていません。 • [Responder]：デバイス上で IP SLA レスポンダのプロファイルが設定されています。このプロファイルで設定されているデバイスは、測定パケットを処理し、タイムスタンプの詳細情報を提供します。 レスポンダは、接続先デバイスの処理遅延に関する情報を、送信元の Cisco ルータに返すことができます。
Cisco Prime Collaboration リリース 11.1 以前の場合 Performance Monitor	• [Unsupported]：デバイスは Cisco Performance Monitor をサポートしません。 • 未設定—デバイスは Cisco Performance Monitor をサポートしますが、設定されていません。 • [Configured]：Cisco Performance Monitor がイネーブルになっているため、ネットワーク内のパケット フローをモニタし、そのフローに影響をおよぼす可能性がある問題点を認識できます。

（注）
- インベントリの不明な電話機を更新するには、Cluster Data Discovery をトリガーします。これは、午前 0 時に自動的にトリガーされます。
- IP アドレスを変更または交換した場合、デバイス タイプは識別されません。このような場合は、
  - */opt/emms/emsam/conf/* フォルダに移動し、*emsam.properties*ファイルを編集します。
  - *com.cisco.nm.emms.devicetype.rediscovery = false* 行を見つけて、値を 'False' から 'True' に変更します。
  - 管理者ユーザとしてログインして Cisco Prime Collaboration Assurance Server を再起動し、
    - **application stop cpcm**
    - **application start cpcm**
  - デバイスの再発見というコマンドを実行します。

Mobile Remote Access（MRA）クライアント（Cisco Jabber、Cisco TelePresence MX シリーズ、Cisco TelePresence System シリーズ、Cisco TelePresence SX シリーズなど）の IP アドレスは Cisco Unified Communications Manager のCisco Expressway-Core デバイスと同じですが、Cisco Prime Collaboration Assurance で IP アドレスは「NA」と表示されます。

（注） デバイス 360° ビューは MRA クライアントで使用できます。

関連トピック

会議の診断ダッシュボード （326 ページ）
デバイス グループの管理 （173 ページ）
Unified CM クラスタ データの検出 （165 ページ）

デバイスの 360° ビュー

360° ビューを使用して、任意のデバイスに関する簡単な概要情報を取得できます。デバイスの IP アドレスの上にマウスを合わせ、クイック ビュー アイコンをクリックして、[デバイス360° ビュー（Device 360° View）] ウィンドウを起動します。デバイスのグローバル検索を実行して、[デバイス360°ビュー（Device 360°View）] を確認することもできます。

ステータスや場所などのデバイス情報の表示に加えて、デバイス上のモジュール、アラーム、インターフェイスの表示や、そのデバイスに対する ping や traceroute などのツールの起動もできます。

デバイスがクラスタに属している場合、クラスタ ID 値をクリックすると、デバイスが属しているクラスタのクラスタ ビューを相互起動できます。

（注） Internet Explorer 10 および 11 を使用している場合は、[デバイス360°ビュー（Device 360° View）] ウィンドウを表示するために推奨されるブラウザ設定を使用していることを確認してください。ブラウザで F12 キーを押して、次のように設定します。

- Internet Explorer 10 の場合：
  - **IE10 ブラウザ モード**：IE10 または IE10 互換表示
  - **ドキュメント モード**：標準（デフォルト）または互換
- Internet Explorer 11 の場合：
  - **ブラウザ プロファイル**：デスクトップ
  - **ドキュメント モード**：Edge（デフォルト）

ブラウザを再度起動して、[デバイス360°ビュー（Device 360° View）] ウィンドウを表示します。

[デバイス360°ビュー（Device 360° View）] ウィンドウには、次のデバイスの詳細が表示されます。

表 *19* : フィールド/ボタンとその説明

フィールド	説明
状態	デバイスの状態を確認するには、状態アイコンにマウスのカーソルを合わせます。アイコンの各色は、さまざまな状態を表しています。
ステータス理由	デバイスのステータス理由と、すべての機能を動作させるために実行する必要がある追加のアクティビティを確認するには、アイコンの上にマウスのカーソルを合わせます。アイコンの各色は、デバイスの状態に対応しています。
ホスト名	—
ホスト IP /グローバル IP アドレス	IP アドレスをクリックすると、[デバイス管理（Device Management）] ページが起動します。ルータとスイッチにログインするには、その IP アドレスをクリックして、TELNET や SSH などの端末クライアント アプリケーションを関連付ける必要があります。 この機能は、MSP モードでは使用できません。
MAC アドレス	デバイスの MAC アドレス。
タイプ	デバイス タイプまたはデバイスのプライマリ ロールまたは機能は、hostname 行の下の右隅に明記されます。たとえば、Finesse、Unified CM または Unity Connection などです。
ホスト名 （Host Name）	NAT 環境で Cisco Prime Collaboration Assurance を MSP モードで展開した場合は、デバイスのホスト名が表示されます。
顧客	Cisco Prime Collaboration Assurance を MSP モードで展開した場合、デバイスが属しているカスタマーを参照することができます。
バージョン	デバイスのソフトウェア バージョン。
最終検出	最後に成功した検出のタイムスタンプです。

フィールド	説明
クラスタ ID	デバイスが属しているクラスタのクラスタ ID です。クラスタ ID をクリックすると、[クラスタの詳細（Cluster Details）] ページが開きます。
—	サポートコミュニティアイコンをクリックすると、デバイスに関連する投稿およびディスカッションがフィルタ処理された シスコ サポートコミュニティ ダイアログボックスが開きます。そのデバイスに関する質問を投稿できます。 他のデバイスのサポートページに移動したり、Cisco Prime Collaboration Assurance のサポートコミュニティ ページにアクセスできます。Cisco Prime Collaboration Assurance ページにアクセスするには、[シスコ サポート コミュニティにアクセス（Visit the Cisco Support Community）] をクリックし、[コミュニティトピックと投稿に移動（Navigate to a Community Topic and Post）] ペインをクリックしてから、[コラボレーション、音声およびビデオ（Collaboration, Voice and Video）] をクリックします。[コラボレーション、音声およびビデオ コミュニティ（Collaboration, Voice and Video Communities）] テーブルで、[Prime Collaboration Management] をクリックします。 Cisco Prime Collaboration コミュニティ フォーラムでは質問を投稿できるほか、既存のディスカッション、動画、関連ドキュメントで問題に関連する質問や情報を検索できます。 ビジネスに影響を及ぼす技術的な問題については、タイムリーなサポートを受けられるよう、Cisco TAC でサービス リクエストを開始することをお勧めします。
—	[ping] アイコンをクリックしてデバイスに ping すると、送受信されたパケットの数、パケット損失（%）、および ping でデバイスに到達するまでの所要時間（ミリ秒）など、ping の統計情報を取得できます。

フィールド	説明
—	[traceroute] アイコンをクリックして、デバイスに到達するためのルート、デバイスに到達するまでのホップ数、および各ホップの経過時間（ミリ秒）を確認します。
—	[タスク（tasks）] アイコンをクリックし、ドロップダウン リストから選択して、パフォーマンス グラフの起動やしきい値の管理などの複数のタスクを実行します。 （注） 使用可能なオプションは、選択したデバイスによって異なります。

その他のデバイス固有の情報は、次のとおりです。

表 *20 :* デバイス *360°* ビュー（*Device 360° View*）：タブの説明

タブ	説明
アラーム	ここでは、次の項目について説明します。 • 重大度：アラームの重大度 • ステータス：アラームのステータス • 名前：デバイスの名前 • コンポーネント：アラームがあるコンポーネントの名前 • 最終更新日：最後のアラーム生成のタイムスタンプ

タブ	説明
インターフェイス	インターフェイス、音声インターフェイス、ポートに関する詳細情報が含まれます（デバイスに該当する場合）。カードが特定のポートで再生されていることと、カードの機能を指定します。インターフェイス、音声インターフェイス、およびポートでは、次の情報を利用できます。 • オペレーションのステータス（Oper Status）：デバイスの動作状態 • 管理ステータス（Admin Status）：インターフェイスの管理ステータス • 名前：デバイスの説明 • アドレス：デバイスの物理アドレス • Type：デバイス タイプ
カード/サービス	ここでは、次の項目について説明します。 • 名前：音声またはサービスの説明 • バージョン：カードまたはサービスのバージョン • ステータス：カードまたはサービスのステータス
ポート	—
環境	内容は次のとおりです。 • 電源モジュール • ファン • 温度センサー • 電圧センサー
デバイス固有の詳細	—

デバイスの [エンドポイント360°ビュー（Endpoint 360° View）] の [接続の詳細（Connectivity Details）] タブの下の Cisco TelePresence TX の Differentiated Services Code Point（DSCP; DiffServ コードポイント）値（10 進形式とその意味の両方）を表示できます。

を選択します。**[インベントリ管理（Inventory Management）]**[IPアドレス（IP Address）] 列をクリックして、[エンドポイント360°ビュー（Endpoint 360° View）] を起動します。

Cisco Prime Collaboration リリース 11.5 以降の場合

選択 **[インベントリ（Inventory）]** > **[インベントリ管理（Inventory Management）]**[IPアドレス（IP Address）] 列をクリックして、[エンドポイント360°ビュー（Endpoint 360° View）] を起動します。

Differentiated Services Code Point（DSCP; DiffServ コードポイント）値の詳細については、RFC 2474 を参照してください。

（注） 表示されるフィールドは、選択したデバイスによって異なります。

上部にある [詳細情報（View More）] ボタンをクリックして、次の操作を行います。

- [デバイス360°ビュー（Device 360°View）] ポップアップをウィンドウサイズで表示する。
- Cisco Unified Communication のアプリケーションまたは固有のカウンタを選択することによって、パフォーマンスダッシュボードを作成できます。詳細については、「「カスタム パフォーマンス ダッシュボードの作成」」を参照してください。

メトリック グラフ

音声デバイス（電話を除く）と CTS のメトリック グラフを表示できます。これらのグラフは、少なくとも 1 つのポーリング サイクルが終了している、管理状態のデバイスのみに表示されます。

（注） デバイスが管理状態になった後、グラフが表示されるまで時間がかかります。これは、グラフのデータを取得するにはポーリングを完了する必要があるためです。

これらのグラフには、CPU、メモリ、ハードディスク使用率などの値が表示されます。最後の 1 時間の最大値、最小値、および現在値（% またはバイト数（MB））を表示できます。メトリック グラフの各棒は 4 分間を表します。棒は 15 本あり、各棒は 4 分の値を表しています。茶色の図は最小値を表し、青色の図は過去 1 時間の最大値を表します。

[詳細を表示（See More）] をクリックすると、一部のデバイスのパフォーマンス グラフが起動します。

マルチポイント コントローラ（MCU）の場合、パフォーマンス グラフで、音声ポートとビデオ ポートの使用率の絶対値とパーセンテージが表示されます。これらのオプションはグラフの右上あたりで選択できます。

TP サーバでは、パフォーマンス グラフを利用できます。絶対値とパーセンテージを確認できます。

（注） メトリック グラフとパフォーマンス グラフが利用できるかどうかは、選択したデバイスによります。

Cisco Prime Collaboration Assurance のグローバル検索オプション

Cisco Prime Collaboration リリース 11.6 および 12.1 の場合

次の表では、Cisco Prime Collaboration Assurance のグローバル検索オプションについて説明します。

表 *21 : Cisco Prime Collaboration Assurance* のグローバル検索オプション

検索	変数	ストリングのフォーマット例	例外および使用できる検索文字列
エンドポイント	DN	10002|1000*| 100*| 1*| *0002	英数字、ダッシュ、ピリオド、アンダースコアを使用します。
	IP	10.64.101.162 | 10.64.101.* | * 10.78.22.77| . | 10.78.22.*| 10.78.*.*| 10.*.*.*| *.	英数字、ダッシュ、ピリオド、アンダースコアを使用します。特殊文字 % は結果を取得しません。 アンパサンド（&）とスペースは使用できません。
	MAC	00260bd75cf8| 00260bd75cf*| 00260bd*| 0*| 00*	ダッシュ、ピリオド、アンダースコアは使用できません。英数字と空白スペースは使用できます。 （注） グローバル検索オプションで MAC アドレスを使用して電話機を検索する場合、コロン、ハイフン、ドットは使用しないでください。
	エンドポイント名	San Jose	-

検索	変数	ストリングのフォーマット例	例外および使用できる検索文字列
デバイス	IP	10.78.22.129| 10.78.22.*| 10.*	英数字、ダッシュ、ピリオド、アンダースコア、スペースを使用します。
	DNS	cussmtest-15.cisco.com	ドメイン名が解決可能でない場合は、IPアドレスが検索結果に表示されます。
ユーザ	名 または 姓 または ユーザ名	HS John	英数字、ダッシュ、アンダースコア、空白スペースは使用できません。

Cisco Prime Collaboration リリース 11.6 および 12.1 の場合

検索結果

検索パラメータ	検索結果
エンドポイント	エンドポイント名、ディレクトリ番号、IP アドレス、IPv6 アドレス、MACアドレス、モデル、クラスタ名、ソフトウェアバージョン、登録ステータス、ステータス理由が表示されます。エンドポイント検索を実行すると、すべての電話機と Cisco TelePresence エンドポイントが検索されます。 IP アドレスの横にあるアイコンをクリックすると、エンドポイントの [エンドポイント 360 ビュー（Endpoint 360 View）] が起動します。
デバイス	名前、IP アドレス、ステータス、デバイス タイプが表示されます。デバイス検索を実行すると、すべての電話機と Cisco TelePresence エンドポイントが検索されます。 デバイス名の横にあるアイコンをクリックすると、デバイスの [エンドポイント 360 ビュー（Endpoint 360 View）] が起動します。 （注）　表示される情報は、検索したデバイスによって異なります。
ユーザ	名、姓、ユーザ名が表示されます。デバイス名の横にあるアイコンをクリックすると、ユーザの [ユーザ 360° ビュー（User 360° View）] が起動します。

Cisco Prime Collaboration Assurance を MSP モードで導入した場合は、検索したデバイスが属する顧客を参照することもできます。デバイスが複数の顧客に属する場合は、そのデバイスが属するすべての顧客が表示されます。デバイスが顧客に関連付けられていない、またはすべての顧客に関連付けられている場合、そのデバイスはデフォルトの顧客ドメイン、つまりすべての顧客に含まれていますが、検索結果の顧客の詳細では空白が表示されます。顧客名をクリックすると、その顧客でフィルタリングしたホームページを起動できます。

ユースケースの検索

次のユースケースに基づき、検索を実行できます。

表 *22 :* ユースケースの検索

検索：	実行/使用
特定の顧客に属するすべてのデバイスです。	画面の右上にある [グローバル顧客の選択] ドロップダウン リストから顧客を選択して、次に [デバイスの検索（Device Search）] を選択し、検索文字列を入力します *。
Cisco Jabber	エンドポイント検索
E20	エンドポイント検索
インフラストラクチャ デバイス	デバイスの検索
部分的な IP アドレスを持つデバイスの IP アドレスです。	デバイスの検索：とえば、10 などの文字列で検索するとします。*
特定の顧客に関連付けられているすべてのユーザの一覧です。	画面の右上にある [グローバル顧客の選択] ドロップダウン リストから顧客を選択して、次に [ユーザの検索（User Search）] を選択し、検索文字列を入力します *。

インベントリの概要

[インベントリの概要（Inventory Summary）] には、デバイスの数がデバイスの状態に基づいて表示されます。[合計（Total）] 列には、特定の状態にあるデバイスの合計数が表示されます。デバイス数からは、[インベントリ管理（Inventory Management）] の [インベントリ（Inventory）] テーブルをクロス起動できます。デバイス数をクリックすると [インベントリ（Inventory）] テーブルが表示され、その特定の状態にあるすべてのデバイスを確認できます。

[インベントリの概要（Assurance Inventory Summary）] は、ユーザ インターフェイス ブラウザの下部にスライダとして用意されています。下へスクロールすると詳細を表示できます。[インベントリの概要（Assurance Inventory Summary）] のデータは、30 秒ごとに更新されます。

表 *23 : [*インベントリの概要（***Inventory Summary***）*]* - フィールドの説明

フィールド	説明
不明なエンドポイント	不明なエンドポイントの合計数。この数をクリックすると、[エンドポイントの診断（Endpoint Diagnostics）] ページで、不明なエンドポイントのフィルタ処理されたリストを開くことができます。
Partially Managed	管理対象状態にあるものの、一部のクレデンシャルが不足しているデバイスの数。これらのクレデンシャルは、インベントリの管理には必須ではありませんが、トラブルシューティングなど、他のあらゆる機能を正しく実行するために必要となります。対応する数をクリックすると、インベントリ テーブルをクロス起動して、管理対象でありながらクレデンシャルが不足しているすべてのデバイスの一覧を確認できます。この数は、クレデンシャルの追加後に再検出を実行した場合にのみ更新されます。

（注） [合計数（Total Count）] 列には、[インフラストラクチャデバイス（Infrastructure Devices）]、[エンドポイント（TelePresence Endpoints）] 列をデバイスの状態ごとに合計した値が含まれますが、[合計数（Total Count）] 列のデバイス数には多少の不整合が生じることがあります。このような差異は、インベントリから不明な状態のデバイス タイプが計算に含められた場合に発生します。

デバイス ステータスの概要

Cisco Prime Collaboration リリース 11.5 以降の場合

[デバイス ステータスの概要（Device Status）] には、デバイスの数がデバイスの状態に基づいて表示されます。電話機や不明なデバイスはカウント数に含まれません。デバイスのカウントは、[インベントリ管理（Inventory Management）] の [インベントリ（Inventory）] テーブルに対するクロス起動として使用できます。デバイス数をクリックすると[インベントリ（Inventory）] テーブルが表示され、その特定の状態にあるすべてのデバイスを確認できます。カウントは、顧客/Assuranceドメインに基づいて絞り込むことができます。

[デバイス ステータスの概要（Device Status Summary）] は以下で使用できます。 **[インベントリ（Inventory）]** > **[デバイス ステータスの概要（Device Status Summary）]**。**[デバイス（Devices）]** 列には、特定の状態にあるデバイスの合計数が表示されます。**[ステータス（Status）]** 列には、デバイスのステータスが表示されます。**[ディスカバリ ジョブ（Discovery**

Jobs）] をクリックすると **[ジョブの管理（Job Management）]** ページに移動し、ディスカバリ ジョブのステータスが表示されます。

次のデバイス ステータスが表示されます。ステータスの詳細については、『*Cisco Prime Collaboration Assurance* ガイド- *Advanced*』の「「ディスカバリ ライフ サイクル」」セクションを参照してください。

- 管理対象（Managed）
- Partially Managed
- Inaccessible
- Unreachable
- Suspended
- Unsupported
- Undiscoverable

[Partially Managed]、[Inaccessible]、[Undiscoverable] 状態にマウスを合わせると、説明を含むツール チップを表示できます。

[インベントリの概要（Inventory Summary）] の横にあるグローバル サマリー バーには、[Unmanaged] デバイスの数が表示されます。数をクリックすると、**[デバイス ステータスの概要（Device Status Summary）]** ページに移動します。

表 *24* : デバイス ステータスの概要 - フィールドの説明

フィールド	説明
デバイスの検出ステータス	デバイスの検出ステータスを表示します。
進行中のデバイス検出 <カウント>	検出が実行されているデバイス数を表示します。検出が行われていない場合、進行中のデバイス検出 <カウント> は表示されません。

Cisco Prime Collaboration リリース 12.1 以降の場合

[デバイス ステータスの概要（Device Status）] には、デバイスの数がデバイスの状態に基づいて表示されます。この表で示されたとおり、デバイスにはインフラストラクチャ コンポーネントやビデオ/TelePresence のエンドポイントが含まれています。電話機はカウントされません（DX シリーズを含みます）。数をクリックすると、**[インベントリ管理（Inventory Management）]** ページのインベントリ テーブルに移動し、特定の状態にあるすべてのデバイスが表示されます。カウントは、顧客/Assuranceドメインに基づいて絞り込むことができます。

[デバイス ステータスの概要（Device Status Summary）] を利用するには、**[インベントリ（Inventory）]** > **[デバイス ステータスの概要（Device Status Summary）]** の順に選択します。**[デバイス（Devices）]** 列には、特定の状態にあるデバイスの合計数が表示されます。**[ステータス（Status）]** 列には、デバイスのステータスが表示されます。

[ディスカバリ ジョブ（Discovery Jobs）] をクリックすると **[ジョブの管理（Job Management）]** ページに移動し、ディスカバリ ジョブのステータスが表示されます。

次のデバイス ステータスが表示されます。ステータスの詳細については、『Cisco Prime Collaboration Assurance ガイド- Advanced』の「ディスカバリ ライフ サイクル」セクションを参照してください。

デバイス ステータスの概要データは、[Managed] と [Unmanaged] の 2 つのカテゴリに分類されます。

- [Managed] カテゴリは、次のとおりです。
  - Discovered Successfully
  - Partially Managed
- [Unmanaged] カテゴリは、次のとおりです。
  - Inaccessible
  - Unreachable
  - Suspended
  - Unsupported
  - Undiscoverable
  - Unknown

[Partially Managed]、[Inaccessible]、[Unreachable]、[Undiscoverable] 状態にマウスを合わせると、説明を含むツール チップを表示できます。

両方のカテゴリ（[Managed] と [Unmanaged]）の数は、それぞれのカテゴリの合計デバイス数と一致する必要があります。

[インベントリの概要（Inventory Summary）] の横にあるグローバル サマリー バーには、[Unmanaged] デバイスの数が表示されます。この数は、**[デバイス ステータス（Device Status）]** テーブル内の [Unmanaged] デバイスの数と一致する必要があります。数をクリックすると、**[デバイス ステータスの概要（Device Status Summary）]** ページに移動します。

表 *25 :* デバイス ステータスの概要 - フィールドの説明

フィールド	説明
デバイスの検出ステータス	デバイスの検出ステータスを表示します。
進行中のデバイス検出 <カウント>	検出が実行されているデバイス数を表示します。検出が行われていない場合、進行中のデバイス検出 <カウント> は表示されません。

トラブルシューティング

問題：CUCM の再検出によりCisco Prime Collaboration Assurance インベントリから Pub が消滅します。これは、CUCM 上で共存する ELM/PLM 設定が原因です。Cisco Prime Collaboration Assurance は大文字と小文字を区別するため、ELM/PLM 設定は CUCM のホスト名と一致する必要があります。

たとえば、CUCM 上で共存する ELM/PLM 設定のホスト名が lax-ccm-px.apl.com であり、CUCM のホスト名が LAX-CCM-PX.apl.com である場合、CUCM Pub の再検出を実行すると、CUCM Pub はインベントリから消滅するか、削除されます。

推奨アクション：Cisco Prime Collaboration Assurance の **/etc/hosts** ファイルを変更し、CUCM Pub を再検出します。次に示されたとおり、ホスト ファイルにエントリを追加します。

10.8.2.20	LAX-CCM-PX.apl.com

インベントリ ステータスのエラー メッセージ

クレデンシャル検証のエラー メッセージを次の表に示します。

表 *26* : クレデンシャル検証のエラー メッセージ

エラー メッセージ	状態	解決策
SNMP_ERROR	次のいずれかの原因により失敗します。 • デバイスで SNMP サービスが有効である • SNMP クレデンシャルが一致しません。 • ファイアウォールの設定によってポートがブロックされています。	• デバイスで SNMP サービスが有効かどうか確認する • クレデンシャル プロファイルで、デバイスの SNMP クレデンシャルを確認して再入力します。 • ファイアウォールの設定によってポートがブロックされていることを確認し、適切なポートを使用してポートのブロックを解除します。必要なポートの詳細については、「Prime Collaborationに必要なポート」を参照してください。
UNKNOWN_ERROR	デバイスの検出中にエラーが発生します。	再検出を実行します。問題が解決しない場合は、TAC に連絡してサポートを受けてください。

エラー メッセージ	状態	解決策
INSUFFICIENT_INV_COLLECTION	デバイスの応答時間が予想よりも長い場合は、ネットワーク遅延が発生している可能性があります。	SNMP/HTTP(S) の応答時間を確認し、再検出を実行します。問題が解決しない場合は、TAC に連絡してサポートを受けてください。
HTTP_ERROR	HTTP アクセスに失敗します。次のいずれかの原因により失敗します。 • HTTP(S) クレデンシャルが一致しない • ファイアウォールの設定によってポートがブロックされています。	• クレデンシャル プロファイルで、デバイスの HTTP クレデンシャルを確認して再入力します。 • ファイアウォールの設定によってポートがブロックされていることを確認し、適切なポートを使用してポートのブロックを解除します。必要なポートの詳細については、「Prime Collaborationに必要なポート」を参照してください。

エラー メッセージ	状態	解決策
JTAPI_ERROR	JTAPI アクセスに失敗しますファイアウォールの設定によってポートがブロックされています。	• クレデンシャル プロファイルで、デバイスの JTAPI クレデンシャルを確認して再入力します。 （注） パスワードにはセミコロン（;）や等号（=）を使用しないでください。 • ファイアウォールの設定によってポートがブロックされていることを確認し、適切なポートを使用してポートのブロックを解除します。必要なポートの詳細については、「Prime Collaborationに必要なポート」を参照してください。 • JTAPI ユーザが Cisco Unified CM で設定されているかどうか確認します。JTAPI を有効にするための詳細については、「Prime Collaboration Assurance 用にデバイスを設定」を参照してください。
aUNSUPPORTED_DEVICE	デバイスがサポートされていません。	サポートされているデバイスを「Cisco Prime Collaboration Assurance でサポートされているデバイス」で確認します。
UNDISCOVERABLE	エラーが続きます。	再検出を実行します。問題が解決しない場合は、TAC に連絡してサポートを受けてください。

エラー メッセージ	状態	解決策
DISCOVERY_FAIL_TOO_MANY_DB_CONNECTIONS	エラーが続きます。	再検出を実行します。問題が解決しない場合は、TAC に連絡してサポートを受けてください。

デバイス固有のインベントリ詳細

次の表に、追加のインベントリの詳細を説明するフィールドの説明を示します。

- 表 27 : Cisco Codec、MX, E20、MXP
- 表 28 : Cisco TelePresence Movi
- 表 29 : Cisco Unified IP Phone 8900 および 9900 シリーズ
- 表 30 : CTMS
- 表 31 : Cisco TMS
- 表 32 : Cisco Unified CM
- 表 33 : Cisco MCU および MSE
- 表 34 : Cisco VCS
- 表 35 : Cisco TelePresence Conductor

表 *27 : Cisco Codec*、*MX, E20*、*MXP*

フィールド		説明
TelePresence Endpoint （選択したエンドポイント タイプの CTS、Cisco Codec、MX、E20、MXP、に基づいてデータが表示されます）	エンドポイント名	識別を容易にするためにエンドポイントに割り当てられた名前。
	電話番号	エンドポイントで定義されている IP 電話の詳細です。
	コール コントローラ	
	CUCM アドレス	エンドポイントが登録されている、Cisco Unified CM サーバのホスト名または IP アドレスです。
	CUCM クラスタ ID	Cisco Unified CM サーバが登録されている Cisco Unified CM クラスタの IDです。
	VCS アドレス	エンドポイントが登録されている VCS サーバのホスト名または IP アドレスです。
	VCS クラスタ ID	VCS サーバが登録されている VCS クラスタの ID です。
	登録ステータス	コール プロセッサ（Cisco Unified CM または VCS）でのエンドポイントの登録ステータスです。Cisco Unified CM または VCS が管理対象ではない場合は、表示される情報は [N/A] です。
	H323 ID	Cisco Codec デバイスで設定されている H.323 ID です。
	E164 No	

フィールド		説明
		Cisco Codec デバイスで設定されている E164 番号です。
	H323 ゲートキーパー アドレス	Cisco Codec デバイスが登録されているゲートキーパーのネットワーク アドレスです。
	SIP URI	Cisco Codec デバイスで登録されている SIP URI です。
	SIP プロキシ アドレス	Cisco Codec デバイスで手動設定されている SIP プロキシ アドレスです。
	アプリケーション マネージャ	
	TMS	Cisco Codec デバイスが統合されているアプリケーションマネージャのホスト名または IP アドレスです。
	スイッチの詳細	
	スイッチに接続済み	エンドポイントが接続されているスイッチの詳細です。
	接続済みポート	エンドポイントが接続されているスイッチ ポートの詳細です。
	周辺機器	名前

フィールド		説明	
			アップリンク、電話機、カメラ、ディスプレイ、タッチ スクリーン モニタ、マイクなどのペリフェラルのタイプ。
位置		マイクの *front_center* など、周辺機器の位置です。	
MAC アドレス		周辺機器の MAC アドレスです。	
ソフトウェア バージョン		ペリフェラルで実行されているソフトウェア バージョンです。	
モデル		周辺機器のモデルです。	
シリアル		周辺機器のシリアル番号です。	
製造元		周辺機器の製造元の詳細です。	
ファームウェア バージョン		周辺機器のファームウェア バージョンです。	
ハードウェア バージョン		周辺機器のハードウェア バージョンです。	
Midlet バージョン		周辺機器で実行されている Midlet バージョンです。	

（注） Cisco Prime Collaboration Assuranceは、Cisco TelePresence 150 MXP のペリフェラルの詳細をサポートしていません。

表 *28 : Cisco TelePresence Movi*

フィールド		説明
Movi	エンドポイント名	識別を容易にするためにエンドポイントに割り当てられた名前。
	SIP URI	Cisco TelePresence Movi エンドポイントで登録されている SIP URI です。
	VCS アドレス	エンドポイントが登録されている VCS のホスト名または IP アドレスです。
	VCS クラスタ ID	VCS が登録されている VCS クラスタの ID です。

表 *29 : Cisco Unified IP Phone 8900* および *9900* シリーズ

フィールド		説明
CUCM エンドポイント	エンドポイント名	識別を容易にするためにエンドポイントに割り当てられた名前。
	モデル	CP-8945 や CP-9971 などのエンドポイントのモデルです。
	電話番号	エンドポイントで定義されている IP 電話の詳細です。
	シリアル番号	エンドポイントのシリアル番号です。
	説明	コール プロセッサで定義されているエンドポイントの説明です。
	コール コントローラ	
	CUCM アドレス	エンドポイントが登録されている、Cisco Unified CM サーバのホスト名または IP アドレスです。
	CUCM クラスタ ID	Cisco Unified CM サーバが登録されている Cisco Unified CM クラスタの ID です。
	登録ステータス	コール プロセッサ（Cisco Unified CM）でのエンドポイントの登録ステータスです。Cisco Unified CM が管理対象ではない場合は、表示される情報は [N/A] です。
	スイッチの詳細	
	スイッチに接続済み	エンドポイントが接続されているスイッチの詳細です。
	接続済みポート	エンドポイントが接続されているスイッチ ポートの詳細です。

フィールド		説明
ステータス	接続や未接続などの Wi-Fi 接続のステータスを表示します。	
IP アドレス	Wi-Fi ネットワークを使用して接続する際に、エンドポイントの管理に使用する IP アドレスです。	
デフォルト ルータ	エンドポイントが接続されているデフォルト ルータの IP アドレスです。	
アクセス ポイント名	エンドポイントが接続されているアクセス ポイントの名前です。	
イーサネットの詳細		
ステータス	接続や未接続などのイーサネット接続のステータスを表示します。	
IP アドレス	イーサネットを使用して接続する際に、エンドポイントの管理に使用する IP アドレスです。	

（注） Cisco Unified IP Phone 8900 および 9900 シリーズの検出には、HTTP インターフェイスを有効にする必要があります。HTTP インターフェイスが有効になっていない場合は、これらのデバイスはインベントリ テーブルに表示されません。

表 *30 : CTMS*

フィールド		説明
マルチポイント スイッチ	タイムゾーン	マルチポイント スイッチで設定されたタイム ゾーンです。
	SKU	—
	ハードウェア モデル	マルチポイント スイッチが実行されているメディア コンバージェンス サーバの型番です。
	ソフトウェア バージョン	管理ソフトウェアが現在インストールしているマルチポイント スイッチのバージョン。
	OS バージョン	オペレーティング システムのバージョンです。
	ホスト名	マルチポイント スイッチに設定されているホスト名。
	IP アドレス	マルチポイント スイッチの管理に使用される IP アドレスです。
	サブネット マスク	IP アドレスで使用されるサブネット マスクです。
	MAC アドレス	マルチポイント スイッチ ソフトウェアが実行されているメディア コンバージェンス サーバのMACアドレスです。このMACアドレスは、イーサネット インターフェイス 0（eth0 ネットワーク インターフェイス カード（NIC））に属します。フェールオーバーでは、この MAC アドレスは、別のイーサネット インターフェイスがアクティブになっても保持されます。
	スイッチの詳細	
	スイッチに接続済み	

フィールド		説明
		マルチポイント スイッチが接続されるスイッチの詳細です。
	接続済みポート	マルチポイント スイッチが接続されるスイッチ ポートの詳細です。
	アドホック セグメント	緊急会議で使用可能なセグメントの最大数です。最大値は 48 です。
	最大セグメント	このマルチポイント スイッチが処理できるセグメント（個々のビデオ ディスプレイ）の合計数です。最大値は 48 です。
	スケジュール設定可能	スケジュール済み会議で常に使用できるセグメントの数。マルチポイント スイッチは、定義された最大セグメント数から、定義されたアドホック セグメントの数を引くことにより、この値を自動的に導出します。

表 *31 : Cisco TMS*

フィールド		説明
アプリケーション マネージャ	SKU	—
	ハードウェア モデル	アプリケーション マネージャが実行されているサーバの型番です。
	ソフトウェア バージョン	現在インストールされている管理ソフトウェアのバージョンです。
	OS バージョン	オペレーティング システムのバージョンです。
	ホスト名	アプリケーション マネージャに設定されているホスト名。
	IP アドレス	アプリケーション マネージャの管理に使用される IP アドレス。
	サブネット マスク	IP アドレスで使用されるサブネット マスクです。
	MAC アドレス	アプリケーション マネージャに提供されるMACアドレス番号です。

フィールド		説明
システムの接続（この表の後の注を参照）	ステータス	Exchange サーバが実行しているか、ダウン状態かを示します。
	IP アドレス	Exchange サーバに割り当てられる IP アドレスです。
	ソフトウェア バージョン	Exchange サーバに現在インストールされているソフトウェアのバージョン。
	ステータス	LDAP サーバが実行しているか、ダウン状態かを示します。
	IP アドレス	LDAP サーバに割り当てられる IP アドレス。
	ソフトウェア バージョン	LDAPサーバに現在インストールされているソフトウェアのバージョンです。

表 *32 : Cisco Unified CM*

フィールド		説明
[コール プロセッサ（Call Processor）]	クラスタ ID	クラスタの一意のIDを提供するパラメータです。このパラメータは、コール詳細レコード（CDR）で使用されるため、複数のクラスタからのCDR レコード収集はソースに対して追跡できます。デフォルトは StandAloneCluster です。
	パブリッシャ ホスト名	クラスタ パブリッシャに設定されているホスト名です。
	登録済み CTS エンドポイント	コール プロセッサに登録されているエンドポイントの数です。
	合計 CTS エンドポイント	エンドポイントの合計数です。

表 *33 : Cisco MCU* および *MSE*

フィールド		説明
MCU または MSE の詳細 （選択した会議デバイスが MCU か MSE かに基づいてデータが表示されます）	ハードウェア モデル	マルチポイント スイッチが実行されているメディア コンバージェンス サーバの型番です。
	シリアル番号	マルチポイント コントロール ユニット（MCU）のシリアル番号です。
	ソフトウェア バージョン	管理ソフトウェアが現在インストールしているマルチポイント スイッチのバージョン。
	MCU タイプ/デバイス タイプ	MCU またはデバイスのタイプです。
	ビルド バージョン	インストールされたソフトウェアのビルド バージョンです。
	メーカー	製造元の名前です。
	ホスト名	デバイスに設定されたホスト名（MCU または Media Service Engine）。
	IP アドレス	MCU または MSE Web ユーザ インターフェイスへのアクセスに使用する MCU または Media Service Engine（MSE）ネットワーク インターフェイスのローカル IP アドレス。
	サブネット マスク	IP アドレスで使用されるサブネット マスクです。
	MAC アドレス	イーサネット ポートの固定ハードウェア MAC アドレスです。
	ルータに接続済み	MCU または MSE が接続されているルータの IP アドレスです。
	クラスタ タイプ	

フィールド		説明
		クラスタがマスターかスレーブかを示します。クラスタが設定されている場合は、[未設定（Not Configured）] が表示されます。
	ビデオ ポートの合計数	MCUで設定されているビデオポートの数です。（MCUデバイスに対してのみ表示されるデータ）
	音声ポートの合計数	MCU で設定されている音声ポートの数です。（MCUデバイスに対してのみ表示されるデータ）
	SIP（MCU デバイスに対してのみ表示されるデータ）	
	ステータス	SIPの登録がイネーブルかディセーブルかを示します。
	プロキシ	SIP プロキシのネットワーク アドレス。
	ドメイン	MCU が登録されている SIP レジストラのネットワーク アドレス。
	H.323（MCU デバイスに対してのみ表示されるデータ）	
	ステータス	H.323 ゲートキーパーの登録がイネーブルかディセーブルかを示します。
	ゲートキーパー ID	H.323 ゲートキーパーへの登録時に MCU で使用される ID です。
	ゲートキーパー アドレス	MCUが登録されているゲートキーパーのネットワーク アドレスです。

フィールド		説明
MSE ブレード （MSE に対してのみ表示されるデータ）	タイプ	ブレードのタイプです。
	スロット	スロット番号スロット 1 は MSE スーパーバイザです。スロット 2-10 はブレードです。
	ソフトウェア バージョン	使用されているソフトウェアのバージョンです。
	ステータス	ブレードのステータスで、OK または空です。
	Port A IP アドレス	Port A の IP アドレスです。
	Port B IP アドレス	Port B の IP アドレスです。

表 *34 : Cisco VCS*

フィールド		説明
[コール プロセッサ（Call Processor）]	クラスタ ID	別の VCS のクラスタを識別するために使用するクラスタ名です。
	Master	クラスタ マスターとして設定された VCS ピアの名前です。
	登録済みのエンドポイント	VCS に登録されているエンドポイントの数です。
	ピア	クラスタ内で設定されている VCS ピアの数です。

フィールド		説明
VCS Configuration	タイムゾーン	VCS で設定されたタイムゾーンです。
	Maximum Traversal Calls	VCS で利用可能なトラバーサル コール ライセンスの数です。
	Maximum Non-Traversal Calls	VCS で利用可能な非トラバーサル コール ライセンスの数です。
	Maximum Registrations	VCS に登録可能なエンドポイントの数です。
	Expressway	VCS Expressway が設定されているかどうかを示します。
	Interworking	H.323 システムから SIP システムへ接続できるように VCS が設定されているかどうかを示します。
	暗号化	ソフトウェア ビルドで AES 暗号化を使用できるかどうかを示します。
	Find Me	FindMe が有効または無効のどちらになっているかを示します。
	デバイス プロビジョニング	VCS でプロビジョニング サーバがイネーブルかどうかを示します。
	Dual Network Interface	VCS Expressway 上で LAN 2 インターフェイスがイネーブルかどうかを示します。
	Starter Pack	Starter Pack オプション キーがインストールされているかどうかを示します。

（注） Cisco Prime Collaboration Assurance は、Cisco VCS アプリケーションとアプライアンスの両方を管理します。

表 *35 : Cisco TelePresence Conductor*

フィールド		説明
TelePresence Conductor	名前	コンダクタに設定されたホスト名です。
	IP アドレス	コンダクタの IP アドレスです。
	ソフトウェア バージョン	現在インストールされているソフトウェアのバージョン
	Cluster Master	クラスタ マスターとして設定されたコンダクタ ピアの名前。
	Cluster Peers	クラスタ内で設定されているコンダクタ ピアの数。
	Total Registered MCUs	コンダクタに登録されている MCU の数。
	ソフトウェア ID	コンダクタ上のソフトウェアの ID。
	ハードウェアのシリアル番号	コンダクタ ハードウェアのシリアル番号。

フィールド		説明
Registered MCUs	名前	コンダクタに登録されている MCU の名前。
	IP アドレス	コンダクタに登録されている MCU の IP アドレスです。
	タイプ	コネクタに登録されている MCU のタイプです。
	Pool	MCU クライアントが属する MCU プール。
	Blacklisted	リストされた MCU はコンダクタでは使用されません。
	Blacklisted Reason	その MCU がコンダクタで使用されない理由。
	Media Load: Allocated/In Use/ Max Available	メディア ロードが割り当てられた、使用中、および使用可能な最大ロード。
	Signalled Load: Allocated/In Use/ Max Available	シグナル ロードが割り当てられた、使用中、および使用可能な最大ロード。

（注） Cisco TelePresence Conductor が制御する MCU のカスケードのみがサポートされます。

Cisco Prime Collaboration リリース 11.5 以降の場合

（注） 次のデバイスはサポートされていません。

- Cisco TelePresence Multipoint Switch (CTMS)
- Cisco TelePresence-Manager (CTS-MAN)

インベントリ詳細の更新と収集

インベントリの詳細を更新および収集する方法は、音声、ビデオ、またはその両方で導入されたネットワークの種類によって異なります。また、指定されたポイントで収集するデータに

よっても異なります。次の表には、ネットワークに基づきインベントリを更新するタイミングの推奨事項が示されています。

表 *36* : インベントリの更新に関する推奨事項

説明	タスク
ネットワークに音声とビデオの両方のエンドポイントが導入されている場合に、両方のデータを収集します。	インベントリの更新を実行します（**[デバイスインベントリ（Device Inventory）]** > **[インベントリ管理（Inventory Management）]** > **[現在のインベントリ（Current Inventory）]**。詳細については、インベントリの更新を参照してください。 **Cisco Prime Collaboration リリース 11.5 以降の場合** 選択 **[インベントリ（Inventory）]** > **[インベントリ管理（Inventory Management）]** > **[インベントリの更新（Update Inventory）]**
音声とビデオの両方のエンドポイントがネットワークに導入されており、ビデオのエンドポイントのみでデータを収集します。	インベントリの更新を実行します（**[デバイスインベントリ（Device Inventory）]** > **[インベントリ管理（Inventory Management）]** > **[インベントリの更新（Update Inventory）]**。詳細については、インベントリの更新を参照してください。 **Cisco Prime Collaboration リリース 11.5 以降の場合** 選択 **[インベントリ（Inventory）]** > **[インベントリ管理（Inventory Management）]** > **[インベントリの更新（Update Inventory）]**
音声とビデオの両方のエンドポイントがネットワークに導入されており、音声のエンドポイントのみでデータを収集します。	を実行します（を選択します）。**保証管理（Assurance Administration）**。詳細については、インベントリ詳細の収集を参照してください。 **Cisco Prime Collaboration リリース 11.5 以降の場合** 選択 **アラーム & レポート管理**。

説明	タスク
音声ネットワークのみを使用している場合	クラスタ データの検出を実行します（を選択します）。**保証管理（Assurance Administration）**。詳細については、インベントリ詳細の収集を参照してください。 **Cisco Prime Collaboration リリース 11.5 以降の場合** 選択 **アラーム & レポート管理**。
ビデオ ネットワークのみを使用している場合	インベントリの更新を実行します（**[デバイスインベントリ（Device Inventory）] > [インベントリ管理（Inventory Management）] > [インベントリの更新（Update Inventory）]**。詳細については、インベントリの更新を参照してください。 **Cisco Prime Collaboration リリース 11.5 以降の場合** 選択 **[インベントリ（Inventory）] > [インベントリ管理（Inventory Management）] > [インベントリの更新（Update Inventory）]**

インベントリの更新

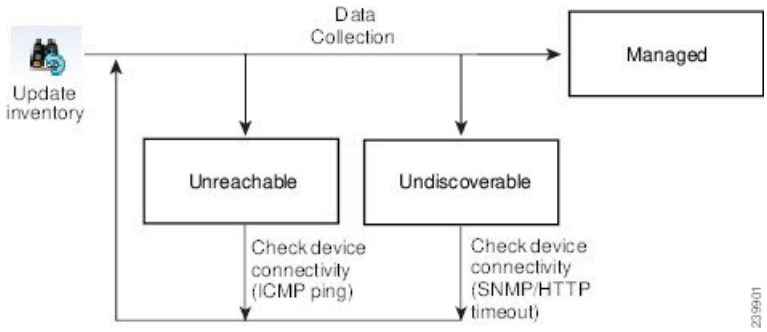
Update Inventory タスクを使用すると、Cisco Prime Collaboration Assurance のインベントリ データベースをネットワークに同期することができます。このタスクでは、アクセシビリティの検証が実行されません（「Update Inventory のライフサイクル」の図を参照）。

次の場合に Update Inventory タスクを実行します。

- ネットワークで管理されているすべてのデバイスのデータベースを同期する必要がある場合。ただし、デバイス ステータス基準に基づいて、特定のデバイスの詳細な構成を更新することができます。
- Cisco Prime Collaboration Assurance データベースを最新の状態に保つために、定期的な Update Inventory ジョブを定義する必要がある場合。
- ネットワークデバイスのインターフェイスに変更がある場合。

（注） ネットワークに追加された新しいデバイスは特定されません。

図 *3 : Update Inventory* のライフサイクル



Cisco Prime Collaboration Assurance データベースを最新の状態に保つために、定期的な Update Inventory を定義することを推奨します。

インベントリを更新するには、次の手順を実行します。

ステップ 1 を選択します。**[デバイスインベントリ（Device Inventory）]** > **[インベントリ管理（Inventory Management）]**。

Cisco Prime Collaboration リリース 11.5 以降の場合

移行方法 **[インベントリ（Inventory）]** > **[インベントリ管理（Inventory Management）]**

ステップ 2 **インベントリ管理** ページで、**[インベントリの更新(Update Inventory）]** をクリック します。

ステップ 3 デバイスのステータスに基づいてインベントリを更新する場合は、[インベントリの更新（Update Inventory）] ウィンドウの [デバイスの条件に基づいてデバイスを更新する（Update devices based on device criteria）] チェックボックスをオンにし、ドロップダウン リストから必要なデバイスの条件を選択します。

デバイスのステータスに基づいてインベントリを更新するように選択した場合、アクセシビリティ情報のチェックが実行されます。この選択を行わない場合、管理状態のすべてのデバイスでインベントリが更新されます。デバイスのアクセシビリティはチェックされません。

定期的なインベントリ更新ジョブのスケジュールを設定するには、**ステップ 4** を追加で実施します。ジョブをただちに実行するには、**ステップ 5** に進みます。

ステップ 4 ジョブ名とスケジュールの詳細を入力します。フィールドの説明については、「ジョブ スケジュール - フィールドの説明」を参照してください。

ステップ 5 [今すぐ実行（Run Now）] をクリックしてインベントリ更新ジョブをすぐに実行するか、[スケジュール（Schedule）] をクリックして定期的なインベントリ更新ジョブをスケジュールします。

ステップ 6 ジョブのステータスを確認するには、次のいずれかを実行します。

- [今すぐ実行（Run Now）] をクリックする場合は、表示される進行状況ウィンドウで進捗状況の詳細をクリックします
- [] [インベントリ管理（Inventory Management）] ページの **[検出ジョブ（Discovery Jobs）]** ボタンをクリックします。

ジョブ スケジュール - フィールドの説明

表 *37:* ジョブ スケジュール - フィールドの説明

フィールド	説明
Start Time	[開始時刻（Start Time）] を選択して、開始の日時を *yyyy/MM/dd* および *hh:mm AM/PM* の形式で入力します。あるいは、日付ピッカーをクリックして、カレンダーから開始の日時を選択します。表示される時刻は、クライアントのブラウザの時刻です。スケジューリングされた定期的ジョブは、この指定時刻に実行されます。
繰り返し	[なし（None）]、[毎時（Hourly）]、[毎日（Daily）]、[毎週（Weekly）]、[毎月（Monthly）] のいずれかを選択し、ジョブの期間を指定します。
設定	ジョブ期間の詳細です。
終了時刻	終了日時を指定する必要がない場合は、[終了日時なし（No End Date/Time）] をクリックします。終了日時を *yyyy/MM/dd* と *hh:mm AM/PM* の形式で入力するには、[終了（End at）] をクリックします。

インベントリ詳細の収集

Cisco Prime Collaboration Assurance は、管理対象デバイスに登録されたデバイスと電話に関するデータを収集および更新することによって、管理対象デバイスのオンデマンドインベントリ更新をサポートします。

電話、XML 電話、クラスタのすべての追加、削除、および変更は、インベントリに反映されます。電話機とクラスタには、個別のインベントリ収集スケジュールがあります。クラスタ検出の詳細については、「Unified CM クラスタ データの検出」を参照してください。

追加のスケジュールは作成できません。編集できるのは、既存のスケジュールのみです。電話機の場合は、複数のインベントリ収集スケジュールを作成できます。

（注） Cisco Unified CM クラスタの定期的な検出のみをスケジュールできます。他のクラスタに登録された電話は検出されません。詳細については、「Unified CM クラスタ データの検出」を参照してください。

Cisco Prime Collaboration Assurance によって電話や Cisco Unified CM クラスタのインベントリ収集が実行されるときに、これらの電話やクラスタはさまざまなデバイス状態を経て Cisco Prime Collaboration Assurance によって完全に認識されます（詳細については、「ライフ サイクルの検出」を参照してください）。

インベントリ収集で管理される電話機およびクラスタに関する情報を収集する頻度を指定できます。インベントリ収集のスケジュールを設定するには、を選択します。**保証管理（Assurance Administration）**。

Cisco Prime Collaboration リリース 11.5 以降の場合

[インベントリ収集（Inventory Collection）] をスケジュールするには、**[アラームとレポートの管理（Alarm & Report Administration）]**を選択します。

インベントリ収集タスクの概要については、次の表を参照してください。

表 *38* : インベントリ収集タスクの概要

タスク	説明
クラスタ デバイスのインベントリ収集のスケジュール設定	**Cisco Prime Collaboration リリース 12.1 以降の場合** **[インベントリ（Inventory）] > [クラスタ データ検出のスケジュール（Cluster Data Discovery Schedule）]** クラスタ デバイス検出スケジュールを追加、編集、または削除するには(詳細については、クラスタ デバイスの検出をスケジュール （166 ページ）を参照してください)

管理対象デバイスの一時停止と再開

管理対象状態のデバイスを一時停止できます。デバイスを一時停止状態に入った後は、Cisco Prime Collaboration Assurance によってこのデバイスが監視されることはありません。つまり、会議、エンドポイント、およびインベントリの詳細は更新されず、このデバイスに対するアラームはトリガーされません。

次に、一時停止状態のデバイスの動作を示します。

- デバイスが一時停止状態の場合、Cisco Prime Collaboration Assurance によってデバイスはポーリングされません。
- 一時停止中のエンドポイントが新しい会議に参加すると、そのエンドポイントは、[会議（Conference）] [トポロジ（Topology）] ペインに [不明（Unknown）] として表示されます。
- 一時停止中のエンドポイントがすでに進行中の会議にある場合は、エンドポイントの状態が [一時停止（Suspended）] に変更された直後に、エンドポイント アイコン（[会議（Conference）] [トポロジ（Topology）] ペイン内）） が [不明（Unknown）] に変わります。

- Cisco Unified CM Publisher が一時停止されている場合、対応する Cisco Unified CM クラスタに属する登録済みのエンドポイントは、Cisco Prime Collaboration Assurance によってポーリングされません。
- アクティブアラームがある場合、すぐにはクリアされません。手動でアラームをクリアするか、期限切れ（デフォルトは 24 時間）後に自動的にクリアされます。一時停止されたデバイスでは、新しいアラームはトリガーされません。
- 現在のクラスタに対してバックグラウンドジョブ（エンドポイントの同期、電話 XML など）が実行されている場合は、CUCM デバイスを削除することができません。
- **Cisco Prime Collaboration リリース 11.1 以前の場合**

  一時停止されたエンドポイントがトラブルシューティングジョブにある場合、一時停止されたエンドポイントからトラブルシューティングを実行することはできません。ただし、一時停止されたエンドポイントまでトラブルシューティングを実行できます。
- デバイスが一時停止された場合、Endpoint Utilization レポートには、このデバイスのデータは含まれません。
- **Cisco Prime Collaboration リリース 12.1 SP2 以降の場合**

  TC/CE エンドポイント管理ステータスが「管理対象」から「一時停止」に変更された場合は、登録を解除する必要があります。

管理対象デバイスを一時停止または再開するには:

ステップ 1 を選択します。**[デバイスインベントリ（Device Inventory）]** > **[インベントリ管理（Inventory Management）]**。

Cisco Prime Collaboration リリース 11.5 以降の場合

移行方法 **[インベントリ（Inventory）]** > **[インベントリ管理（Inventory Management）]**

ステップ 2 [Current Inventory] テーブルから、管理対象または一時停止デバイスで選択します。

ステップ 3 [Suspend] または [Resume] をクリックします。

ステップ 4 確認メッセージ ボックスで [OK] をクリックします。

（注） 削除オプションを使用してインベントリから電話機を直接削除することはできません。電話機が登録されたクラスタが削除されると、電話機も自動的に削除されます。インベントリは、再検出の実行後にのみ更新されます。

デバイスの削除

状態が [Unknown]、[Unreachable]、[Inaccessible]、[Undiscoverable]、[Suspended]、[Unsupported] のデバイスは削除できます。[管理対象（Managed）] 状態のデバイスは削除できません。

デバイスは削除された後、[現在のインベントリ（Current Inventory）] テーブルには表示されませんが、詳細は Cisco Prime Collaboration Assurance サーバで参照できます。削除されたデバイスを再検出するには、「デバイスの再検出」 を参照してください。過去の会議データの一部として、削除されたデバイスの詳細にアクセスできます。

Cisco Prime Collaboration リリース 12.1 以降の場合

状態が [Unknown]、[Unreachable]、[Inaccessible]、[Undiscoverable]、[Suspended]、[Unsupported] のデバイスは削除できます。[管理対象（Managed）] 状態のデバイスは削除できません。

デバイスは削除された後、[現在のインベントリ（Current Inventory）] テーブルには表示されませんが、

古い IP エントリを含むエンドポイントを DEVICE_REMOVED フィードバックの一部として削除し、新しい IP エントリ（VCS の新しいエンドポイントとして見なされる）を別途追加する必要があります。

Cisco Prime Collaboration リリース 12.1 SP2 以降の場合

TC/CE エンドポイントがインベントリから削除された場合は、HTTPS フィードバック サブスクリプションがエンドポイントから削除されます。

削除状態でのデバイスの動作を次に示します。

1. 現在のクラスタに対してバックグラウンド ジョブ（エンドポイントの同期、電話 XML など）が実行されている場合は、CUCM デバイスを削除することができません。
2. Cisco Prime Collaboration Assurance では、すべての同時セッションに対して一度に 1 つの削除要求のみ実行可能です。他のセッションからデバイスまたはエンドポイントを削除しようとすると、「同時実行の削除操作がバックグラウンドで実行されています。しばらくしてからもう一度お試しください（Concurrent delete operation is running in background, please try after sometime）」というメッセージが表示されます。
3. Cisco Prime Collaboration Assurance では、いったん削除または削除されたデバイス情報は保持されません。デバイス管理ステータスで DELETED 状態ではなくなります。

デバイスを削除する手順は、次のとおりです。

ステップ 1 を選択します。**[デバイスインベントリ（Device Inventory）]** > **[インベントリ管理（Inventory Management）]**。

Cisco Prime Collaboration リリース 11.5 以降の場合

移行方法 **[インベントリ（Inventory）]** > **[インベントリ管理（Inventory Management）]**

ステップ 2 [現在のインベントリ（Current Inventory）] テーブルから、削除するデバイスを選択します。

クイック フィルタを使用して、対象とする状態のデバイスのリストを取得できます。

ステップ 3 [Delete] をクリックします。

ステップ 4 確認メッセージ ボックスで [OK] をクリックします。

（注） 削除オプションを使用してインベントリから電話機を直接削除することはできません。電話機が登録されたクラスタが削除されると、電話機も自動的に削除されます。インベントリは、再検出の実行後にのみ更新されます。

トラブルシューティング

問題：Managed の状態のデバイスは削除できません。

推奨処置：まずデバイスが一時停止されていることを確認してから、デバイスを削除してください。

パフォーマンス グラフ

Cisco Prime Collaboration Assurance ではネットワーク パフォーマンス メトリックを選択し、変更を確認できます。収集されたデータ以外に、ネットワーク パフォーマンス データをリアルタイムに選択、表示、図化することができます。

パフォーマンス グラフには、、、[アラームとイベント（Alarm & Events）] ページ、[デバイス 360°（Device 360°）] ビュー、[診断の概要（Diagnostic Summary）] ページからアクセスできます。次の場合に、現在またはリアルタイムのデータからパフォーマンス グラフを作成できます。

- デバイスの音声使用率ポーリングがイネーブル
- デバイスは管理状態です。

（注） パフォーマンス グラフを表示できるのは、音声デバイス（電話機を除く）のみが対象です。表示されるグラフは、管理状態にあり、少なくとも 1 つのポーリング サイクルが含まれているデバイスのみが対象です。

パフォーマンス グラフに関する特記事項

この項では、パフォーマンス グラフを使用する場合の注意事項について説明します。

概要	説明
シスコでは、最適なパフォーマンス グラフ ビューに関する次のガイドラインに従うことを推奨します。	次のガイドラインが推奨されます。 • 1 つのグラフに対して 5 メトリック以下にします。 • ユーザインターフェイスには 10 個以下のグラフにします。 • マージには 10 項目以下を選択します。
Catalyst 6000 スイッチ上の MGCP ゲートウェイ。3 種類すべての機能（音声ゲートウェイ、スイッチ、MGCP）がある場合は、パフォーマンス グラフではすべてのデータをグラフ化できません。代表的なメトリックだけがグラフで使用できます。	3 種類の機能（音声ゲートウェイ、スイッチ、MGCP）を備えたデバイスのパフォーマンス メトリックをグラフ化するときは、代表的なメトリックだけがグラフ化できます。[Event Details] ページには、HighUtilization イベントをグラフ化できません。
音声ゲートウェイ、MGCP、およびルータの H323。1 つのデバイスにこの 3 種類すべての機能がある場合は、メトリック別に 2 種類のグラフを表示します。	これら 3 種類の機能（音声ゲートウェイ、MGCP、ルータの H323）を持つデバイスのパフォーマンス メトリックをグラフ化する場合、メトリック別に 2 種類のグラフを表示します。また、複数のデバイスまたは複数のポーリング間隔を持つデバイスをグラフ化する場合、少なくとも 2 つ以上の共通のポーリング間隔で x 軸をプロットします。リアルタイムでグラフ化すると、この共通のポーリング間隔でリフレッシュされます。
Cisco Unity Express サーバ（CUES）は、リアルタイム データをグラフ化し、リアルタイムで更新します。折れ線から棒グラフに切り替え、特定のデータを拡大して、トラブルシューティングを実行し、ピーク使用率の期間を検索できます。	Cisco Prime Collaboration Assurance がデータを収集し、このデータを受信するよう適切に設定されていることを確認します。

パフォーマンス グラフの起動

次の項目からパフォーマンス グラフを使用できます。

- [デバイス 360 度（Device 360 degree）] ビュー：[起動ツール（Launch Tools）] アイコンをクリックし、[パフォーマンス グラフ（Performance Graph）] をクリックします。
- Event Details ページ
- 診断ビュー：UCM クラスタ コール使用概要のサーバおよびクラスタ ビュー、UCM リソース使用率概要および UCM クラスタ ロケーション概要のクラスタ ビュー、ならびにトラ

ンク使用率は、UCM リソース使用率概要ポートレットのクラスタ ビューを介してアクセスできます。

始める前に

- Cisco Prime Collaboration Assurance が、使用率統計を収集するデバイスを監視していることを確認します。これには、ポートが登録されている Cisco Unified Communications Manager も含まれます。
- 音声使用のポーリング設定が有効になっていることを確認します。Cisco Prime Collaboration Assurance は、ネットワーク パフォーマンスをグラフ化するため、音声使用のポーリング中に収集した統計を使用します。
- パフォーマンス グラフの注釈を確認します。

パフォーマンス グラフ ウィンドウ

パフォーマンス グラフでは、リアルタイム情報と履歴情報を提供します。

パフォーマンス グラフを起動すると、選択したメトリックごとに 1 行のグラフが表示されます。各折れ線グラフには、リアルタイムで表示される 16 個のデータ ポイントがあります。次の表には、データ オプションの詳細が示されています。

グラフ データ オプション	説明
Real Time	パフォーマンス グラフを起動すると、デフォルトではリアルタイム データが表示されます。
Hourly Average	[毎時平均（Hourly Average）] を選択すると、パフォーマンス グラフには時間の平均データが表示されます。
Hourly Max	[毎時最大（Hourly Max）] を選択すると、パフォーマンス グラフには時間の最大データが表示されます。
Hourly Min	[毎時最小（Hourly Min）] を選択すると、パフォーマンス グラフには時間の最小データが表示されます。
履歴	[履歴（History）] を選択すると、パフォーマンス グラフには 7 日間の毎時平均データが表示されます。
すべて	すべてのデータが表示されます。グラフには、最大 130 ポイントが表示されます。ズーム/パン ビューのデータ範囲に 130 ポイント以上含まれている場合、Cisco Prime Collaboration Assurance は一定の間隔をあけてポイントを選択し、グラフにプロットします。

パフォーマンス グラフのトラブルシューティング

この項には、パフォーマンス グラフ生成時に発生した問題の解決に役立つ情報が含まれています。エラーが発生した場合は、メニューの [パフォーマンスのグラフ作成（Performance Graphing）] を選択した場合、または Cisco Prime Collaboration Assurance がグラフ化するデータファイルの確認中に表示されます。前者の（Performance Graphing を選択した）場合は、問題と対処法が記されたエラー メッセージが表示されます。次の表には、この 2 つのタイプのケースでエラーおよび考えられる原因が示されています。

エラー	考えられる原因

データを収集できません	• アカウントおよびクレデンシャルがクラスタ内のすべての Cisco Unified Communications Managers で同一ではありません。
	• HTTP サーバの問題：
	  • デバイスの HTTP サーバがダウンしています。
	  • HTTP サーバは動作しているが、Cisco Unified Communications Managers がダウンしています。
	• ネットワークの問題でデバイスに到達できません。
	• **Cisco Prime Collaboration リリース 11.1 以前の場合**
	メディア サーバでパフォーマンス モニタリングのプロセスがダウンしています。
	• MGCP ゲートウェイが登録されている Cisco Unified Communications Manager は、Cisco Prime Collaboration Assurance インベントリにはありません。
	• デバイスの機能がサポートされていません。パフォーマンスのグラフ化では、Cisco Unity、Cisco Unity Express、Cisco Unified Communications Manager、Cisco Unified Communications Manager Express、、H.323 デバイス、Voice Mail Gateway がサポートされています。
	• デバイスが一時停止しているか削除されています。
	• デバイスのプラットフォームがサポートされていません。
	サポートされているデバイスの一覧については、「Cisco Prime Collaboration Assurance でサポートされているデバイス」を参照してください。

エラー	考えられる原因
次の理由により、データを収集できません。 • デバイスのユーザ名またはパスワードが指定されていません。 • システムが保有するデバイスのクレデンシャルが正しくありません。 • デバイスにクレデンシャル情報がありません。	• Cisco Prime Collaboration Assurance にクレデンシャルがありません。 • Cisco Prime Collaboration Assurance のクレデンシャルが正しくありません。 クレデンシャルを追加するには、**「デバイス クレデンシャル プロファイルの追加」**を参照してください。。
次の理由により、デバイスからデータを収集できません。 • 処理エラーが発生しました。 • 解析または処理エラーが発生しました。 • 内部で初期化エラーが発生しました。 • デバイスのデータ コレクタで初期化エラーが発生しました。	Cisco Unified Communications Manager のバージョンが正しくありません。次の点を確認します。 • デバイスで実行している Cisco Unified Communications Manager バージョンを確認します。 • Cisco Prime Collaboration Assurance に格納されている Cisco Unified Communications Manager バージョン番号を確認します。 • Cisco Prime Collaboration Assurance に格納されている Cisco Unified Communications Manager バージョン番号が正しくない場合は、デバイスをもう一度追加します。 サポートされているデバイスの一覧については、「Cisco Prime Collaboration Assurance でサポートされているデバイス」を参照してください。
デバイスからデータを収集できません。認証のホスト名/IP アドレスを URL のホスト名/IP アドレスにマップでません。	デバイスが DNS 内にありません。

エラー	考えられる原因
デバイスとの通信でエラーが発生したためにデータ収集が完了しません。	Cisco Unified Communications Manager のバージョンが正しくありません。次の点を確認します。 • デバイスで実行している Cisco Unified Communications Manager バージョンを確認します。 • Cisco Prime Collaboration Assurance に格納されている Cisco Unified Communications Manager バージョン番号を確認します。 • Cisco Prime Collaboration Assurance に格納されている Cisco Unified Communications Manager バージョン番号が正しくない場合は、デバイスをもう一度追加します。 サポートされているデバイスの一覧については、「Cisco Prime Collaboration Assurance でサポートされているデバイス」を参照してください。
次の理由により、データを収集できません。 • デバイスが、必要な MIB からデータを戻しませんでした。 • デバイスは MIB データを受信しませんでした。	• 必要な MIB からのデータがありません。 • 必須 MIB がデバイスに入力されていません。 • MIB の戻りデータがありません。 • ネットワーク障害が原因でデバイスが到達不能です。 • デバイスのクレデンシャルに有効な SNMP コミュニティ リード ストリングが含まれていません。 • SNMP の応答が低速化しています。データ収集がタイムアウトしました。
• Cisco Unified Communications Manager の照会レートが上限を超えました。 • データ処理の段階でエラーが発生しました。	Cisco Unified CM 6.0 以降で実行された照会が多すぎます。 ポーリング設定を確認し、3 分未満である必要があります。

エラー	考えられる原因
• Cisco Unified Communications Manager が照会リクエストを処理する時間が足りませんでした。 • データ処理の段階でエラーが発生しました。	Cisco Unified CM 6.0 以降で実行された照会で、処理時間の上限が超過しました。
Cisco Unity または Unity Express のトランク使用率グラフが機能していません。	Cisco Prime Collaboration Assurance は、最大容量を使用して適切に設定する必要があります。

パフォーマンス グラフを使用する場合は、次のことに注意してください。

- パフォーマンス データを収集できず、エラー メッセージ（ポップアップ メッセージまたはログ ファイルのメッセージ）も表示されない場合は、デバイスのステータスを確認する必要があります。これを行うには、[デバイスの表示/再検出/削除（View/Rediscover/Delete Devices）] ページを使用します。デバイスが到達不能状態の場合は、デバイスのクレデンシャルが正しいことを確認し、デバイスを再検出します。
- グラフに灰色の線または灰色の領域が表示されている場合は、その上にマウス カーソルを合わせると、説明が記載されたツール ヒントを取得できます。

Unified CM デバイスの検索

ユーザが指定した検索条件に基づいて、クラスタ内のデバイスを検索できます。

Cisco Prime Collaboration Assurance を MSP モードで展開した場合は、検索結果がグローバル カスタマー選択に応じて異なります。

Cisco Prime Collaboration リリース 11.5 以降の場合

デバイス検索を実行するには、**[インベントリ（Inventory）]** > **[UC デバイスの検索（UC Device Search）]**の順に移動します。[保存済み検索（Saved Search）] ドロップダウンリストから選択された保存済みの検索条件に基づいて、デバイスを表示できます。

（注） テーブルには、200 個のエントリのみが表示されます。したがって、目的の結果を確実に得るには、フィルタ条件を最大限に使用することを推奨します。

新しい検索条件を作成するには：

ステップ 1 Cisco Prime Collaboration リリース 11.5 以降の場合

移行方法 **[インベントリ（Inventory）]** > **[UC デバイスの検索（UC Device Search）]**。

ステップ 2 [クラスタ（Cluster）] ドロップダウン リストからクラスタを選択します。

[クラスタ（Cluster）] ドロップダウン リストでデバイスを検索することもできます。

ステップ 3 **[New Search]** をクリックします。

ステップ 4 基準名、デバイス タイプ、およびポーリング間隔を入力します

DB オプションに設定されたデバイスだけを選択すると、デバイス タイプを除くポーリング間隔またはその他のパラメータを指定できません。このオプションには不明な状態のデバイスが表示されます。

同じユーザが同じクラスタに同じ検索基準名を使用することはできません。同じユーザが別のクラスタにこの条件名を使用することはできます。

ステップ 5 カスタム検索については、CallManager、デバイス モデル、およびネーム パラメータによる検索内のステータスを指定します。

使用できる検索条件は、選択したデバイス タイプによって異なります。

ステップ 6 [Search] をクリックします。

検索結果がページに表示されます。結果がユーザ指定のポーリング間隔に基づいて更新されます。[IP Address] 列で使用できる IP アドレスのリンクから Unified CM を開始できます。

検索結果には、次の情報も含まれます。

- App Info：アプリケーションに関する情報。
- Configuration：これは、H.323 ゲートウェイに適用されます。
- Port/Channel Status：設定されているすべてのポートやチャネル、およびその状態を表示します。ポーリング間隔を設定して、この表示を更新することができます。

検索はデータベースに保存されないため、保存しないとログアウト後にこの検索を復元できません。検索を保存するには、**[保存（Save）]** アイコンをクリックします。

ユーザが保存した検索を編集することもできます。保存されていなくても、ユーザが作成した検索設定を削除できます。編集または削除アイコンを使用して検索を編集または削除できます。ユーザが編集できないフィールドは無効になっています。

SIP トランクの宛先のステータスも表示できます。[デバイス タイプ] ドロップダウン リストから [SIP トランク] を選択し、[条件名] と [ポーリング間隔] を入力して **[検索]** をクリックします。**[Name]** 列にマウスを合わせてクイック ビューアイコンをクリックし、[送信先の詳細]ポップアップ ウィンドウを表示します。

（注） Internet Explorer 10 または 11 の検索条件を保存するには、ブラウザの [Always Refresh from Server] オプションを有効にする必要があります。このオプションを有効にするには、F12 を押します。Internet Explorer のツールバー メニューで、**[Cache > Always refresh from server]** を選択します。

SNMP クエリ（SNMP Query）

SNMP クエリ機能は、ネットワーク内のデバイスのトラブルシューティングに役立ちます。

次の場合に SNMP クエリを実行します。

- ネットワーク内のデバイスが、Cisco Prime Collaboration Assurance で管理された状態になりません。
- ネットワーク内のデバイスが、およびインベントリ管理の一覧に表示されません。
- SNMP ポーリングが正常に実行されません。

前提条件 - デバイスは、Cisco Prime Collaboration Assurance によってサポートされている必要があります。

サポートされているデバイスの一覧については、「Cisco Prime Collaboration Assurance でサポートされているデバイス」を参照してください。

SNMP クエリを実行するには、次の手順に従います。

1. 選択 **[デバイスインベントリ（Device Inventory）]** > **[SNMP MIB クエリ ツール（SNMP MIB Query Tool）]**。

   Cisco Prime Collaboration リリース 11.5 以降の場合

   移行方法 **[インベントリ（Inventory）]** > **[SNMP MIB クエリ ツール（SNMP MIB Query Tool）]**。

2. IP アドレスを入力して OID ドロップダウン リストから OID タイプを選択し、次のいずれかの操作を実行します。

   - 特定の OID の戻り値を確認するには、[取得（GET）] ボタンをクリックします。たとえば、インターフェイス名やインターフェイス ステータスを確認する場合です。

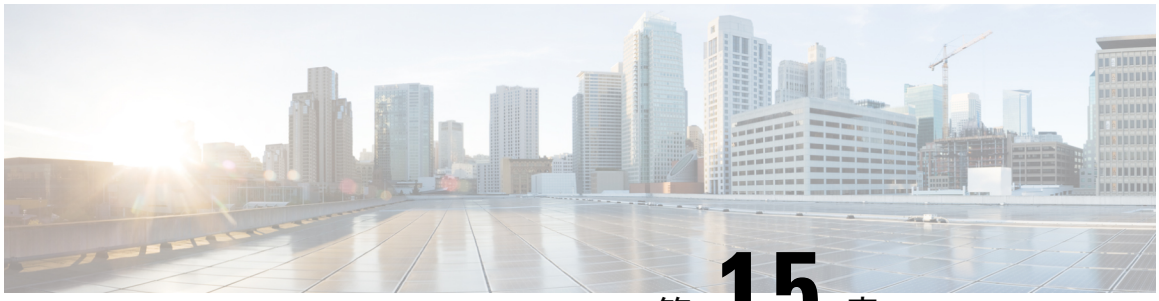
     このタスクを実行するには、クレデンシャルが必要です。Cisco Prime Collaboration でデバイス情報が利用できる場合は、詳細が画面に自動入力されます。それ以外の場合は、[クレデンシャルの入力（Enter the Credentials）] チェックボックスをオンにし、バージョン ドロップダウン リストから SNMP バージョンを選択し、表示されるフィールドに詳細を入力します。
   - 対象デバイスの MIB に関する詳細情報を取得するには、[ウォーク（WALK）] ボタンをクリックします。

     このタスクを実行するには、クレデンシャルが必要です。Cisco Prime Collaboration でデバイス情報が利用できる場合は、詳細が画面に自動入力されます。それ以外の場合は、[クレデンシャルの入力（Enter the Credentials）] チェックボックスをオンにし、バージョン ドロップダウン リストから SNMP バージョンを選択し、表示されるフィールドに詳細を入力します。

   ページには、IOD に関する情報が表で表示されます。

トラブルシューティング - 次の場合、SNMP クレデンシャルは自動入力されません。

- 検出が完了していないため、Cisco Prime Collaboration データベースにはまだクレデンシャルが追加されていない可能性があります。
- デバイスが、およびインベントリ管理で Unknown または Inaccessible 状態になっています。
- デバイスで SNMP クレデンシャルが設定されていません。



第 15 章

ポーリング デバイス

このセクションでは、次の点について説明します。

- ポーリングの設定 （237 ページ）
- 概要 （237 ページ）
- ポーリング パラメータ：設定 （239 ページ）
- ポーリング パラメータの表示 （240 ページ）
- ポーリング パラメータの編集 （240 ページ）

ポーリングの設定

このセクションでは、デバイスのポーリングに使用する設定について説明します。

概要

デバイスを定期的にポーリングすると、デバイスを検出し、正常性を確認します。管理されたネットワーク デバイスは定期的にポーリングされ、デバイス データは Cisco Prime Collaboration Assurance のデータベースと同期されます。

Cisco Prime Collaboration Assurance は、次の目的のためにデバイスをポーリングします。

- デバイスが到達可能であることを確認する
- デバイスが動作していることを確認する
- 最新のデバイス データを表示する

グループのポーリング値を定義できます。デバイスは、システム定義またはユーザ定義のグループに属することができます。デバイスは、複数のグループに所属し、特定のポーリングを設定することもできます。

（注） [Polling Parameters] ページでグループを作成することはできません。グループは、デフォルトのデバイス グループから同期されます。詳細については、デバイス グループ セレクタを参照してください。

Cisco Prime Collaboration Assurance では、ポーリング パラメータはデフォルトで設定されています。デフォルトを使用、編集、またはいつでも復元できます。デバイス グループの重要度に応じてポーリング間隔を変更し、次のいずれかを実行することができます。

- ポーリング対象デバイスへの影響を最小限に抑える。
- 収集データの精度を上げる。

When Cisco Prime Collaboration Assurance がデバイスをポーリングすると、次のパラメータによるデータを受信します。

環境設定

デバイスの電源、ファン、電圧、温度センサーのデータをポーリングします。

インターフェイス設定

HTTP を介したデバイス通信など、デバイス インターフェイスとポートのデータをポーリングします。

インターフェイスとポートからポーリングされたのデータは、デバイス レベルで制御されます。つまり、スイッチには特定のポーリング設定があり、この設定によってスイッチ ポートをポーリングするタイミングが決定します。

システム設定

デバイスの可用性、プロセッサ、CPU、メモリ使用率に関するデータをポーリングします。

使用率

パフォーマンス グラフで表示されるよう、パフォーマンスとキャパシティの計画データを収集します。

パフォーマンス グラフには、、[アラームとイベント（Alarms & Events ）] ページ、、[デバイス 360 度（Device 360 degree）] ビュー、[診断の概要（Diagnostics Summary）] ページからアクセスできます。

アプリケーション設定

デバイス接続、システム ステータス、コール品質用のデータをポーリングします。

サービス設定

サービス設定は、クラスタ接続やテレフォニー設定など、サービスの問題に関するデータを提供します。

ポーリング パラメータは、選択したデバイス タイプによって異なります。

特定のデータをポーリングしない場合は、[無効化（Disable）]オプションを使用してポーリング設定を無効にすることができます。

推奨事項：

- **Cisco Prime Collaboration リリース 11.1 以前の場合**

  パラメータのポーリング間隔は、ビジネス ニーズに基づきカスタマイズできます。ただし、**[ベスト プラクティスの使用（Use Best Practice）]** ラベルが付いたポーリング間隔を使用することを推奨します。それぞれのポーリング設定では、しきい値違反が発生したときに、関連付けられているイベントを表示することもできます（で表示）。**[アシュアランス管理（Assurance Administration）] > [イベントのカスタマイズ（Event Customization）] > [System（システム）]**。の説明とデバイス タイプについては、[Prime Collaboration Assurance でサポートされているアラームとイベント（Supported Alarms and Events for Prime Collaboration Assurance）] ページを参照してください。

  Cisco Prime Collaboration リリース 11.5 以降の場合

  パラメータのポーリング間隔は、ビジネス ニーズに基づきカスタマイズできます。ただし、**[ベスト プラクティスの使用（Use Best Practice）]** ラベルが付いたポーリング間隔を使用することを推奨します。それぞれのポーリング設定では、しきい値違反が発生したときに、関連付けられているイベントを表示することもできます（**[アラームおよびレポートの管理（Alarm & Report Administration）] > [イベントのカスタマイズ（Event Customization）]>[システム（System）]**。イベントの説明とデバイス タイプについては、[Prime Collaboration Assurance でサポートされているアラームとイベント（Supported Alarms and Events for Prime Collaboration Assurance）] ページを参照してください。

- デフォルトのポーリング間隔は 4 分に設定されていますが、1 分に設定することもできます。一部の重要なデバイスに対してのみ、ポーリング間隔を 1 分に設定することを推奨します。すべてのデバイスでポーリング間隔を 1 分に設定すると、パフォーマンスに悪影響を及ぼします。
- 特定のデータをポーリングしない場合は、[無効化（Disable）]オプションを使用してポーリング設定を無効にすることができます。

ポーリング パラメータ：設定

ポーリング パラメータ設定を変更したときに、変更はそのデバイスだけではなく、グループ全体に適用されます。ポーリング パラメータは、、あるいは ページで、[デバイス グループ（Device Group）] を選択すると表示されます。

Polling Parameters ページから、次の作業を行うことができます。

- ポーリング パラメータの表示
- ポーリング パラメータの編集

ポーリング パラメータの表示

デバイス グループのポーリング設定を表示すると、デバイス グループのメンバーであるデバイスを確認できます。また、ポーリングパラメータのデフォルト値と現在値も確認できます。

ポーリング パラメータを表示するには、以下を行います。

ステップ 1 選択 **[アシュアランス管理（Assurance Administration）] > [ポーリング設定（Polling Settings）]**。

Cisco Prime Collaboration リリース 11.5 以降の場合

移行方法 **[アラームおよびレポート管理（Alarm & Report Administration）] > [ポーリング設定（Polling Settings）]**

ステップ 2 ポーリング パラメータを設定できるデバイス グループを選択します。（通常、これはサブグループを含まないデバイス グループです）。

ステップ 3 ポーリング パラメータを確認し終えたら、ウィンドウを閉じます。

ポーリング パラメータの編集

Cisco Prime Collaboration Assurance のポーリング パラメータを編集する場合は、個々のデバイスではなく、デバイス グループに関連付けられている設定を編集します。ポーリングパラメータ（およびしきい値とプライオリティ）に対するすべての変更を終了したら、すべての変更を適用します。

ポーリング パラメータを編集するには、以下の手順を実行します。

ステップ 1 選択 **[ポーリング設定（Polling Settings）]**。

Cisco Prime Collaboration リリース 11.5 以降の場合

移行方法 **[アラームおよびレポート管理（Alarm & Report Administration）] > [ポーリング設定（Polling Settings）]**。

ステップ 2 ポーリング パラメータを設定できるデバイス グループを選択します（通常、これはサブグループを含まないデバイス グループです）。

ステップ 3 編集するポーリング パラメータを選択し、[ポーリング間隔（Polling Interval）] ドロップダウンから適切な値を選択して、[有効化（Enable）] をクリックします。

ステップ 4 編集する各パラメータに対して、次の手順を繰り返します。

a) パラメータ タイプを選択します。

b) 各設定のパラメータを適切に変更します。

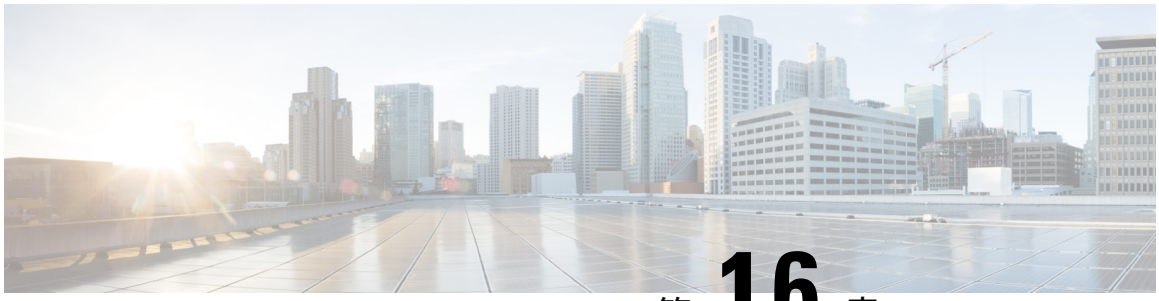
ステップ 5 [保存（Save）] をクリックします。適用するまで変更は反映されません。

ステップ 6 確認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。

第 IV 部

障害のモニタ

- 通知の設定 （245 ページ）
- しきい値ルールの設定 （267 ページ）
- アラームとイベントのモニタリング （289 ページ）



第 16 章

通知の設定

このセクションでは、次の点について説明します。

- 通知の設定 （245 ページ）
- 通知グループ （246 ページ）
- 通知基準 （247 ページ）
- 通知の種類 （248 ページ）
- SNMP トラップ通知 （249 ページ）
- SMTP サーバの設定 （257 ページ）
- syslog 通知 （257 ページ）
- 特定のアラームに制限された通知 （259 ページ）

通知の設定

Cisco Prime Collaboration Assurance では、IP テレフォニー、TelePresence 環境、IP ファブリックで発生するイベントに応答し、イベントやアラーム情報が表示されます。

イベントやアラームは、アラームやイベントのブラウザなど、Cisco Prime Collaboration Assurance ダッシュボードで確認できます。また、他のホストの SNMP トラップ収集装置、syslog 収集装置、およびユーザにイベントに関する情報を転送するように通知を設定することもできます。

通知は、デバイスのコンポーネントではなく、デバイスのロールごとにイベントを監視します。サポートされているイベントとアラームの一覧については、「Prime Collaboration でサポートされているアラームとイベント」を参照してください。

各アラームに対して Cisco Prime Collaboration Assurance は、アラーム、デバイス、重大度、状態を通知が設定されたグループと比較し、一致する場合には通知を送信します。ユーザが設定したアラームセットと通知基準によって一致を決定することができます通知条件を設定する手順については、デバイス通知グループの追加を参照してください。

次の表には、重大度の値と、アラームの状態が時間の経過によってどのように変化するのか示されています。

（注） 通知で送信するイベントの重大度は、Cisco Prime Collaboration Assurance のデフォルト値からユーザ定義の値に変更できます。

この表には、アラーム、イベントの重大度、ステータスが示されています。

表 *39*：アラームとイベントの重大度とステータス

イベント	アラーム
重大度	
• クリティカル 。 • メジャー(Major) • マイナー(Minor) • 警告 。 • 情報：イベントがクリアされると、重大度は情報に変更されます。一部のイベントは、デフォルトで、重大度が [Informational] になっています。	• クリティカル（Critical） • メジャー • マイナー • 警告 • クリア
ステータス（Status）	
• アクティブ - イベントはライブです。 • クリア：イベントはアクティブではありません。	• 認識：ユーザは手動でアラームを認識させています。ユーザは、アクティブなイベントにだけ確認応答を実行できます。 • クリア - アラームはアクティブではありません。 • アクティブ - アラームはライブです。 • User Cleared

通知グループ

通知グループは、通知の生成と送信に関するユーザ定義のルールのセットです。

次の表は、通知先グループの内容について説明しています。

表 *40* : 通知グループ

項目	説明
通知基準	通知が生成される理由の名前付きのセット。
通知タイプ	送信する通知のタイプ。SNMP トラップ、電子メール、または syslog です。
通知の受信者	SNMP トラップ、syslog メッセージ、または電子メール アドレスをリスニングするシステムのホスト名とポート。
毎日の登録アクティビティ期間	Cisco Prime Collaboration Assurance が通知を送信するイベントを監視しているときに、このサブスクリプションを利用すべき時間です。

通知基準

通知基準は、通知を送信するための監視対象項目を定義したものです。通知基準は、デバイスまたは電話、および特定の重大度とステータスを持つイベントのユーザ定義のセットに名前を付けたものです。通知グループを設定するには、通知基準を指定する必要があります。

Cisco Prime Collaboration Assurance は、デバイス ベースの通知条件をサポートします。次の表には、デバイス ベースの通知条件が示されています。

表 *41* : 通知基準

項目	説明
デバイス	モニタするデバイス、デバイス グループ、またはクラスタ。
アラーム セット	(オプション)。モニタする 1 つ以上のアラーム グループ。特定のアラームに制限された通知を参照してください。
アラームの重大度とステータス	複数のアラーム重大度レベルおよびステータス。

また、通知名や、通知によって表示される、特定のアラームに制限された通知デバイス ベース イベントの重大度もカスタマイズできます。

通知の種類

Cisco Prime Collaboration Assurance は、SNMP トラップ、電子メール、syslog という 3 つのタイプの通知を提供します。通知グループを設定するときには、送信する 1 つ以上の通知タイプと、各タイプの通知の受信者を指定する必要があります。

次の表には、通知のタイプが示されています。

表 *42* : 通知タイプ

タイプ	説明
SNMP トラップ通知	Cisco Prime Collaboration Assurance は、アラームとイベントに関するトラップを生成し、トラップの受信者に通知を送信します。これらのトラップは、Cisco Prime Collaboration Assurance サーバによって生成されたイベントとアラームに基づきます。トラップ メッセージの形式は、CISCO-EPM-NOTIFICATION-MIB で定義されています。 SNMP トラップ通知の使用は、Cisco Prime Collaboration Assurance によって処理される前に、rawトラップを別のサーバに転送することではありません。 （注） Cisco Prime Collaboration Assurance は、ポーリングと受信のため、SNMP バージョン 1（SNMPv1）と SNMPv2 トラップをサポートします。Cisco Prime Collaboration Assuranceは、トラップを SNMPv2 トラップとして転送します。ただし、Cisco Prime Collaboration Assurance では、SNMPv3 のトラップ処理はサポートしていません。 MIB OID と、アラームやイベント用として Cisco Prime Collaboration Assurance によって割り当てられる適切な値とのマッピングの詳細については、SNMP トラップ通知を参照してください。

タイプ	説明
電子メール通知	Cisco Prime Collaboration Assurance は、アラーム情報を含む電子メール メッセージを生成します。電子メールの登録を作成するときには、サブジェクト行だけを含めるか、電子メール メッセージ全体を含めるかを選択できます。 （注） Cisco Prime Collaboration Assurance を Enterprise モードでインストールした場合は、件名で次のフォーマットを使用した電子メール通知を受け取ります。
[PC-ALERT-CLUSTERNAME] DEVICE IP : EVENTNAME : SEVERITY. 例： *[PC-ALERT-#CPCM-Ent-Cluster#]50.0.50.230:Gatekeeper Registration Failure:CRITICAL* クラスタ名またはデバイス IP がない場合は、空白である場合があります。	
	NAT 環境では、デバイスのプライベート IP アドレスも表示されます。 Cisco Prime Collaboration Assurance を MSP モードでインストールした場合、デバイスが属しているカスタマーを参照することができます。
Syslog 通知	Cisco Prime Collaboration Assuranceは、リモート システムの syslog デーモンに転送可能なアラーム用の syslog メッセージを生成します。 NAT 環境では、デバイスのプライベート IP アドレスも表示されます。 Cisco Prime Collaboration Assurance を MSP モードでインストールした場合、デバイスが属しているカスタマーを参照することができます。 Syslog メッセージのサンプルと説明については、syslog 通知を参照してください。

SNMP トラップ通知

アラームまたはイベントが Cisco Prime Collaboration Assurance サーバで受信されると、そのサーバは CISCO-EPM-NOTIFICATION-MIB に定義されたトラップ形式に変換されます。他の MIB オブジェクトはサポートされていません。すべてのトラップ レシーバは、同じトラップ フォーマットの同じトラップを受信します。

CISCO-EPM-NOTIFICATION-MIB は、Cisco.com からダウンロードできます。

次の表に、MIB OID とその対応値を、Cisco Prime Collaboration Assurance によってアラームのために割り当てられるものを示します。

表 *43 : CISCO-EPM-NOTIFICATION-MIB* アラーム概要

トラップフィールド名	OID	タイプ	Prime Collaboration のアラーム	トラップ フォワーダの内容（EPM MIB）
cenAlarmIndex	1.3.6.1.4.1.9.9.311.1.1.2.1.1	Unsigned32	-	MIB index
cenAlarmVersion	1.3.6.1.4.1.9.9.311.1.1.2.1.2	SnmpAdmin 文字列	-	この MIB のバージョンです。バージョン文字列は、メジャー バージョン.マイナー バージョンの形式です。 （注） 必ず 9.0 に設定します。
cenAlarmTimestamp	1.3.6.1.4.1.9.9.311.1.1.2.1.3	タイムスタンプ	タイムスタンプ	アラームがトリガーされた時刻です。
cenAlarmUpdated タイムスタンプ	1.3.6.1.4.1.9.9.311.1.1.2.1.4	タイムスタンプ	lastmodified のタイムスタンプ	アラームが最後に変更された時刻です。
cenAlarmInstanceID	1.3.6.1.4.1.9.9.311.1.1.2.1.5	SnmpAdmin 文字列	ID	Cisco Prime Collaboration Assurance によって生成された一意のアラーム ID です。
cenAlarmStatus	1.3.6.1.4.1.9.9.311.1.1.2.1.6	Integer32	lastcleartime	アラームがアクティブであるか（1）、クリアされたか（2）を示します。
cenAlarmStatus 定義	1.3.6.1.4.1.9.9.311.1.1.2.1.7	SnmpAdmin 文字列	lastcleartime	アラームに関する簡単な説明です。 • 1-Active • 2-Cleared
cenAlarmType	1.3.6.1.4.1.9.9.311.1.1.2.1.8	整数	-	アラーム タイプは直接（2）です。
cenAlarmCategory	1.3.6.1.4.1.9.9.311.1.1.2.1.9	Integer32	カテゴリ	アラームのカテゴリ。整数値として表示されます。

cenAlarmCategory 定義	1.3.6.1.4.1.9.9.311.1.1.2.1.10	SnmpAdmin 文字列	カテゴリ	AlarmCategory を文字で表したものです（番号、説明）です。 • 3,Endpoint：すべてのエンドポイントのハードウェア アラーム（ペリフェラル エラー）です。 • 4,Network Devices：すべてのネットワーク デバイスのハードウェア アラーム（インターフェイス エラー）です。 • 5,Service Infrastructure：コールおよび会議制御（Cisco Unified CM および VCS）、管理（ TMS）、マルチポイント スイッチ（CTMS）、およびマルチポイント コントロール ユニット（TPS、MCU）のアラーム。 • 6,Conference：エンドポイントのアラーム（会議の一部）、およびネットワークのアラーム（ジッター、遅延、またはドロップ）。
cenAlarmServer AddressType	1.3.6.1.4.1.9.9.311.1.1.2.1.11	InetAddress タイプ	-	このトラップを生成しているサーバが到達可能なインターネット アドレスのタイプです。この値は、IPv4 管理の場合は 1 に設定されます。
cenAlarmServer アドレス	1.3.6.1.4.1.9.9.311.1.1.2.1.12	InetAddress	-	Cisco Prime Collaboration Assurance IP アドレスです。

cenAlarmManagedObjectClass	1.3.6.1.4.1.9.9.311.1.1.2.1.13	SnmpAdmin 文字列	Source	、Cisco VCS などのソースのエンティティ タイプです。
cenAlarmManagedObjectAddressType	1.3.6.1.4.1.9.9.311.1.1.2.1.14	InetAddress タイプ	ソース	管理対象デバイスが到達可能なインターネットアドレスのタイプです。この値は、IPv4 管理の場合は 1 に設定されます。
cenAlarmManagedObjectAddress	1.3.6.1.4.1.9.9.311.1.1.2.1.15	InetAddress	ソース	管理対象オブジェクトの IP アドレスです。
cenAlarmDescription	1.3.6.1.4.1.9.9.311.1.1.2.1.16	OctetString	説明	アラームの詳細です。
cenAlarmSeverity	1.3.6.1.4.1.9.9.311.1.1.2.1.17	Integer32	重大度	アラームの重大度を整数値で示します。有効な整数は、0-7 です。
cenAlarmSeverity 定義	1.3.6.1.4.1.9.9.311.1.1.2.1.18	OctetString	重大度	アラームの重大度を文字列で表したもの（番号、説明）です。 • 0,critical • 1,major • 2,minor • 3,warning • 4,info • 5,normal • 6,unknown • 7,cleared
cenAlarmTriageValue	1.3.6.1.4.1.9.9.311.1.1.2.1.19	Integer32	-	未使用です。
cenEventIDList	1.3.6.1.4.1.9.9.311.1.1.2.1.20	OctetString	-	このアラームの原因となったイベント ID のリストです。
cenUserMessage1	1.3.6.1.4.1.9.9.311.1.1.2.1.21	SnmpAdmin 文字列	isacknowledged	このアラームが認知されたかどうかを示します。

cenUserMessage2	1.3.6.1.4.1.9.9.311.1.1.2.1.22	SnmpAdmin 文字列	以前の重大度	アラームの以前の重大度。例として、会議の実行中に「メジャー」アラームがトリガーされた場合を考えます。会議が完了すると、会議アラームが自動的にクリアされます。この会議におけるアラームの直前の重大度は「メジャー」であるため、この場合は [メジャー（Major）] と表示されます。
cenUserMessage3	1.3.6.1.4.1.9.9.311.1.1.2.1.23	SnmpAdmin 文字列	-	未使用です。
cenAlarmMode	1.3.6.1.4.1.9.9.311.1.1.2.1.24	整数	-	2：アラート。このトラップは、アラーム通知であるかイベント通知であるかを示します。
cenPartitionNumber	1.3.6.1.4.1.9.9.311.1.1.2.1.25	Unsigned32	-	未使用です。
cenPartitionName	1.3.6.1.4.1.9.9.311.1.1.2.1.26	SnmpAdmin 文字列	-	未使用です。
cenCustomer ID	1.3.6.1.4.1.9.9.311.1.1.2.1.27	SnmpAdmin 文字列	ownerid	Enterprise モードでは、Cisco Prime Collaboration Assurance の通知ユーザインターフェイスに入力された顧客 ID の詳細が表示されます。 MSP モードでは、顧客名が表示されます。
cenCustomer 改定	1.3.6.1.4.1.9.9.311.1.1.2.1.28	SnmpAdmin 文字列	-	未使用です。

cenAlertID	1.3.6.1.4.1.9.9.311.1.1.2.1.29	SnmpAdmin 文字列	id	Cisco Prime Collaboration Assurance によって割り当てられた一意のアラーム ID です。割り当てられているアラーム ID については、「Cisco Prime Collaboration Assurance でサポートされているアラームとイベント」の表を参照してください。

次の表に、MIB OID とその対応値を、Cisco Prime Collaboration Assurance によってイベントのために割り当てられるものを示します。

表 *44 : CISCO-EPM-NOTIFICATION-MIB* イベント概要

トラップ フィールド名	OID	タイプ	Prime Collaboration イベント	トラップ フォワーダの内容（EPM MIB）
cenAlarmIndex	1.3.6.1.4.1.9.9.311.1.1.2.1.1	Unsigned32	-	MIB index
cenAlarmVersion	1.3.6.1.4.1.9.9.311.1.1.2.1.2	SnmpAdmin 文字列	-	この MIB のバージョンです。バージョン文字列は、メジャー バージョン.マイナー バージョンの形式です。 （注） 必ず 9.0 に設定します。
cenAlarmTimestamp	1.3.6.1.4.1.9.9.311.1.1.2.1.3	タイムスタンプ	タイムスタンプ	イベントがトリガーされた時刻です。
cenAlarmUpdatedTimestamp	1.3.6.1.4.1.9.9.311.1.1.2.1.4	タイムスタンプ	-	未使用です。
cenAlarmInstanceID	1.3.6.1.4.1.9.9.311.1.1.2.1.5	SnmpAdmin 文字列	ID	Cisco Prime Collaboration Assurance によって生成された一意のイベント ID です。
cenAlarmStatus	1.3.6.1.4.1.9.9.311.1.1.2.1.6	Integer32	-	未使用です。
cenAlarmStatus 定義	1.3.6.1.4.1.9.9.311.1.1.2.1.7	SnmpAdmin 文字列	-	未使用です。
cenAlarmType	1.3.6.1.4.1.9.9.311.1.1.2.1.8	整数	-	イベント タイプは直接（2）です。

cenAlarmCategory	1.3.6.1.4.1.9.9.311.1.1.2.1.9	Integer32	カテゴリ	イベントのカテゴリです。整数値として表示されます。
cenAlarmCategory 定義	1.3.6.1.4.1.9.9.311.1.1.2.1.10	SnmpAdmin 文字列	カテゴリ	AlarmCategory を文字で表したものです（番号、説明）です。 • 3,Endpoint：すべてのエンドポイントのハードウェアイベント（ペリフェラル エラー）。 • 4,Network Devices：すべてのネットワークデバイスのハードウェアイベント（インターフェイス エラー）。 • 5,Service Infrastructure：コールおよび会議制御（Cisco Unified CM および VCS）、管理（TMS）、マルチポイントスイッチ（CTMS）、およびマルチポイント コントロール ユニット（TPS、MCU）のイベント。 • 6,Conference：エンドポイントのイベント（会議の一部）、およびネットワークのイベント（ジッター、遅延、またはドロップ）。

cenAlarmServer AddressType	1.3.6.1.4.1.9.9.311.1.1.2.1.11	InetAddress タイプ	-	このトラップを生成しているサーバが到達可能なインターネットアドレスのタイプです。この値は、IPv4 管理の場合は 1 に設定されます。
cenAlarmServer アドレス	1.3.6.1.4.1.9.9.311.1.1.2.1.12	InetAddress	-	Prime Collaboration の IP アドレスです。
cenAlarmManaged ObjectClass	1.3.6.1.4.1.9.9.311.1.1.2.1.13	SnmpAdmin 文字列	Source	CTS、Cisco VCS などのソースのエンティティタイプ。
cenAlarmManaged ObjectAddressType	1.3.6.1.4.1.9.9.311.1.1.2.1.14	InetAddress タイプ	ソース	管理対象デバイスが到達可能なインターネットアドレスのタイプです。この値は、IPv4 管理の場合は 1 に設定されます。
cenAlarmManaged ObjectAddress	1.3.6.1.4.1.9.9.311.1.1.2.1.15	InetAddress	ソース	管理対象オブジェクトの IP アドレスです。
cenAlarmDescription	1.3.6.1.4.1.9.9.311.1.1.2.1.16	OctetString	説明	イベントの詳細です。
cenAlarmSeverity	1.3.6.1.4.1.9.9.311.1.1.2.1.17	Integer32	重大度	イベントの重大度を整数値で示します。有効な整数は、0-7 です。
cenAlarmSeverity Definition	1.3.6.1.4.1.9.9.311.1.1.2.1.18	OctetString	重大度	アラームの重大度を文字列で表したもの（番号、説明）です。 • 0,critical • 1,major • 2,minor • 3,warning • 4,info • 5,normal • 6,unknown • 7,cleared
cenAlarmTriageValue	1.3.6.1.4.1.9.9.311.1.1.2.1.19	Integer32	-	未使用です。
cenEventIDList	1.3.6.1.4.1.9.9.311.1.1.2.1.20	OctetString	-	未使用です。
cenUserMessage1	1.3.6.1.4.1.9.9.311.1.1.2.1.21	SnmpAdmin 文字列	-	未使用です。

cenUserMessage2	1.3.6.1.4.1.9.9.311.1.1.2.1.22	SnmpAdmin 文字列	-	未使用です。
cenUserMessage3	1.3.6.1.4.1.9.9.311.1.1.2.1.23	SnmpAdmin 文字列	-	未使用です。
cenAlarmMode	1.3.6.1.4.1.9.9.311.1.1.2.1.24	整数	-	3-event このトラップは、アラーム通知であるかイベント通知であるかを示します。
cenPartitionNumber	1.3.6.1.4.1.9.9.311.1.1.2.1.25	Unsigned32	-	未使用です。
cenPartitionName	1.3.6.1.4.1.9.9.311.1.1.2.1.26	SnmpAdmin 文字列	-	未使用です。
cenCustomer ID	1.3.6.1.4.1.9.9.311.1.1.2.1.27	SnmpAdmin 文字列	-	未使用です。
cenCustomerRevision	1.3.6.1.4.1.9.9.311.1.1.2.1.28	SnmpAdmin 文字列	-	未使用です。
cenAlertID	1.3.6.1.4.1.9.9.311.1.1.2.1.29	SnmpAdmin 文字列	-	未使用です。

SMTP サーバの設定

SMTP サーバ名と送信者 AAA 電子メールアドレスを、**[アラームとイベントの電子メール設定（E-mail Setup for Alarms & Events）]** ページ（**[アラームとレポートの管理（Alarm & Report Administration）]**、> **[アラームとイベントの電子メール設定（E-mail Setup for Alarms & Events）]**）で指定することで、アラームの電子メール通知を送受信するように SMTP サーバを設定することができます。**[Sender AAA E-mail Address]** フィールドの値は、多数のサーバがある場合に、電子メールを受信したサーバを特定するのに便利です。

syslog 通知

syslog メッセージは 1,024 文字までに制限されています（見出しを含む）。この syslog の制限のため、syslog ベースのイベントの詳細には完全な情報が含まれない可能性があります。syslog メッセージがこの制限を超えた場合、syslog の送信側によって 1,024 文字に切り捨てられます。

Cisco Prime Collaboration Assurance server がアラームを送信する際に生成する syslog メッセージの例を、次に示します。

```
Local7.Emerg 10.78.110.27 Feb 19 14:42:49 pcollab-44798 pc798:%local7-0-ALARM:
14$Description=デバイスの温度または温度は通常の動作範囲外です。Out37 イベントが生成されると、通常は、
ファン、電源、電源も表示されます。または温度イベン
ト::Status=1,active^Critical^Acknowledged=no^AlarmURL=https://10.78.110.27/emsam/index.html
 #pageId=com_cisco_ifm_web_page_alarms&queryParams=Id%3D84837&forceLoad=true^Device Work
```

```
 Center=
https://10.78.110.27/emsam/index.html#pageId=com_cisco_emsam_page_inventory&deviceId=3681728
 ^CUSTOMER=customer2/CU44/2,324]。デフォルト アラーム名=Out324^Managed
Object=150.50.3.2^Managed Object Type=Router^MODE=2;アラーム
ID=84837^Component=150.50.3.2/8<000&<000>
```

次の表では、上記の例に基づいて syslog 通知パラメータを説明します。

表 *45 : syslog* 通知の説明

パラメータ	説明
Local7.Emerg 10.78.110.27 Feb 19 14:42:49 pcollab-44798 pcollab-44798	Syslog が生成された Cisco Prime Collaboration Assurance サーバの IP アドレスとホスト名
%local7-0-ALARM	• Syslog Facility データ：%local7 • 重要度：0-深刻、1-重大、2-やや重大、および 3-警告 • タイプはアラーム
14	暦年
説明	アラームの説明
ステータス = 1、アクティブ	アラームのステータス：1 はアクティブ、2 は解除済み
Severity	アラームの重大度
承認済み	アラームが受信確認されているかどうかを示します
AlarmURL	[アラーム（Alarm）] ページを起動する URL
Inventory Management	[インベントリ管理（Inventory Management）] ページを起動する URL
CONFERENCEDIAGNOSTICS	conferencealarm の場合、[会議診断（Conference Diagnostics）] ページを起動する URL
カスタマー	通知の設定中に定義された顧客 ID
CUSTREV	通知の設定中に定義された顧客リビジョン
デフォルト アラーム名	アラーム名
管理対象オブジェクト	アラームが発生したデバイスの IP アドレスまたはホスト名
管理対象オブジェクト タイプ	デバイス タイプ（ルータ、エンドポイントなど）

パラメータ	説明
モード	Syslog メッセージがアラーム (2) であるかどうかを示します
アラーム ID（Alarm ID）	アラームの固有 ID
コンポーネント	アラームが発生したデバイス コンポーネント

特定のアラームに制限された通知

場合によっては、Cisco Prime Collaboration Assurance が監視する一部のアラームのみで、通知を送信する必要があります。目的のアラームは、通知基準を定義するときに、次のように設定することができます。

- デバイスベースの通知基準ごとに、1 つのアラームセットを指定します。アラームセットは必要なだけ作成することができます。

アラーム セットは、次の目的に使用できます。

- Cisco Prime Collaboration Assurance 通知が監視するアラーム数を制限します。アラーム セットを使用しない場合、Cisco Prime Collaboration Assurance 通知はすべてのアラームを監視し、通知を送信するかどうか判断します。
- 異なる複数の宛先に送信する通知の集約。たとえば、次の各目的で個別のアラームセットを作成することができます。
  - 特定の個人または部署に送信される電子メール通知を特定のアラームに関するものだけにして、量を制限する。
  - 特定のアラームの発生をすべて syslog に書き込む。
  - 特定のアラームが発生した場合に SNMP トラップを送信する。

デバイスベースの通知基準を作成する場合は、基準の 1 つとして 1 つのアラーム セットを含める必要があります。デフォルトのアラーム セット「All」には、すべてのアラームが含まれています。

アラーム セットの追加

通知を設定できるアラーム セットを作成できます。

アラーム セットを追加および編集するには、次の手順を実行します。

ステップ 1 選択 **[通知の設定（Notification Setup）]**。

Cisco Prime Collaboration リリース 11.5 以降の場合

移行方法 **[アラームおよびレポート管理（Alarm & Report Administration）] > [通知のセットアップ（Notification Setup）]**

ステップ 2 [カスタム通知（Custom Notification）] をクリックして、詳細を入力します。

（注） 複数のアラームを持つアラームセットを作成する場合、複数の検索基準を使用する必要がある場合があります。このような状況では、[+]アイコンを使用して複数の検索基準を入力する [Advanced Filtering] オプションを使用し、[Match] に [Any] を選択する必要があります。[クイックフィルタ（Quick Filter）] オプションは、思うように動作しない場合があります。

（注） 既存のアラーム セットにアラームを追加する場合は、フィルタリングによって元のアラームのセットが上書きされるのを避けるために、フィルタを使用してアラームを検索しないでください。

ステップ 3 [追加（Add）] をクリックし、必要な情報を指定します。

ステップ 4 [保存（Save）] をクリックして変更内容を保存します。

デバイス通知グループの追加

デバイス通知先グループを追加および編集するには、次の手順を実行します。

（注） 既存の通知グループをテンプレートとして使用し、新しい通知グループを作成することもできます。

ステップ 1 選択 **[通知のセットアップ（Notification Setup）]**[保証通知基準（Assurance Notification Criteria）] を選択します。

Cisco Prime Collaboration リリース 11.5 以降の場合

選択 **[アラームおよびレポート管理（Alarm & Report Administration）] > [通知のセットアップ（Notification Setup）][カスタム通知（Custom Notification）]**を選択します。

ステップ 2 [Add] をクリックして、新しい基準を追加します。

ステップ 3 [新しいデバイスベースの条件（New Device-Based Criterion）] ウィザードで、[一般情報の定義（Define General Information）] ページに次の情報を追加します。

展開モードに基づいて、ドメイン固有または顧客固有のデバイス通知先グループを作成できます。[新しいデバイスベースの条件（New Device-Based Criterion）] ウィザードで、必要な詳細を入力し、[ドメインに関連付け（Associate to Domain）] ドロップダウン リストからドメインを選択するか、[顧客（Customer）] ドロップダウン リストからドメインを選択します。

（注） スーパー管理者はすべてのドメインにアクセスでき、1 つのドメインまたはすべてのドメインの通知グループを作成できます。

ステップ 4 [Next] をクリックします。

[Select Devices/Device Groups] ペインが表示されます。

このチェックボックスをオンにすると、すべてのグループに追加された新しいデバイスが、自動的にそのグループの一部になり、Cisco Prime Collaboration Assurance にデバイスが追加または削除されると、通知基準からも追加または削除されます。このような動作は、該当のデバイスが属するデバイス グループが通知基準に含まれている場合に発生します。

通知基準に含まれるすべてのデバイス グループでデバイスのスタティックなリストを保持する場合は、オフにします。

ステップ 5 [Add] をクリックします。

ステップ 6 [デバイス/デバイスグループの選択（Select Device/Device Groups）] ウィンドウで、[すべてのデバイスを含める（Include all Devices）] または [デバイスの選択（Select Devices）] のラジオボタンをクリックします。

[すべてのデバイスを含める（Include all Devices）] オプションを選択した場合は、デバイス グループ フォルダを展開して、1 つまたは複数のデバイス、デバイスグループ、またはクラスタを選択します。

[デバイスの選択（Select Devices）] オプションを選択した場合は、デバイス グループ フォルダを展開し、1 つまたは複数のデバイス、デバイス グループ、またはクラスタのチェックボックスをオンにします。

（注） クラスタ レベルの電子メール通知を追加する場合は、**[インフラストラクチャ（Infrastructure）]**> **[UCM クラスタ（UCM Clusters）]** デバイス グループ フォルダに一覧表示されているクラスタとクラスタ ID 内のすべてのノードのリストから、クラスタ ID を選択する必要があります。

デバイス グループを選択した場合、[最新情報をグループメンバーシップに含める（Include updates to the group membership）] チェック ボックスをオンにした場合に限り、Cisco Prime Collaboration Assurance からデバイスが追加または削除された時に、通知基準最新の状態に保たれます。すべてのグループに追加された新しいデバイスは、自動的にそのグループの一部になります

ステップ 7 **[Next（次へ）]** をクリックします。

ステップ 8 [通知先の設定（Set up Destination）] ペインで、必要な情報を追加します。

ステップ 9 [Next] をクリックします。

ステップ 10 概要情報を確認し、[Save] をクリックします。

デバイス通知グループを保存すると、[新しいデバイスベースの条件（New Device-Based Criterion）] ウィザードで入力した詳細情報が、[Assurance通知基準（Assurance Notification Criteria）] ページに表示されます。[顧客（Customer）] 列に、通知先グループが所属する顧客が示されます。

[一般情報（General Information）] フィールドの説明

次の表で、[一般情報（General Information）] ウィンドウのフィールドを説明します。

表 *46 :* 一般的情報の追加

グラフィカルユーザインターフェイスの要素	説明
[Criterion Name] フィールド	通知基準の名前を入力します。
[Customer Identification] フィールド	適切な識別情報を入力します。このフィールドが空白のままの場合は、電子メール通知と syslog 通知では空白が表示されます。 SNMP トラップ通知では、次のように表示されます。 `顧客ID: -`
[Customer Revision] フィールド	適切な識別情報を入力します。このフィールドが空白のままの場合は、電子メール通知と syslog 通知では空白が表示されます。 SNMP トラップ通知では、次のように表示されます。 `顧客リビジョン:*`
[Alarm Set Type] リスト ボックス	次のいずれかを選択します。
[Alarm Severity] チェックボックス	オフのままにするか、次の 1 つまたは複数をオンにします。 • 深刻 • やや重大 • 比較的重大でない • 警告
[Alarm Status] チェックボックス	オフのままにするか、次の 1 つまたは複数をオンにします。 • Active • Acknowledged • Cleared • User Cleared

グラフィカルユーザインターフェイスの要素	説明
OperationInterval	通知グループが常にアクティブになるようにスケジュールするには、[Always] オプションボタンをクリックします。 通知グループをアクティブにする時間帯を選択します。 • [From: HH:MM]：登録がアクティブになる時間および分を選択します。 • [To: HH:MM]：登録がアクティブな期間の最後の時間および分を選択します。 デフォルトでは、これらの値は *00:00* から *00:00* までで、登録は24時間アクティブになっています。 たとえば、あるシフトでは電子メール通知を送信し、別のシフトでは送信しないようにする場合にこのフィールドを使用します。

通知先フィールドの説明を設定

次の表に、[通知先の設定（Set up Destinations）] ページのフィールドについて説明します。

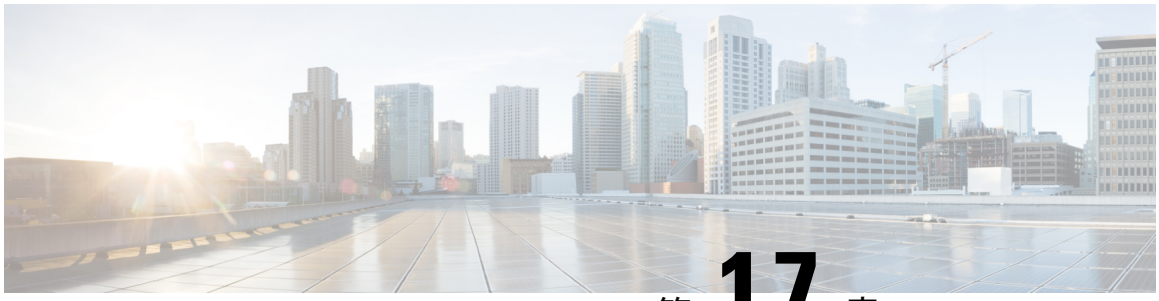
表 *47* : 通知先の設定

グラフィカルユーザインターフェイスの要素	説明
[Include Link to Notification Details] チェックボックス	オンにすると、通知に URL が含まれます。ユーザはその URL を使用して、関連する詳細な情報を確認するためのページを Cisco Prime Collaboration Assurance で直接開くことができます。 通知から URL を省略する場合はオフにします。

グラフィカルユーザインターフェイスの要素	説明
[Subscription Type] オプション ボタン	該当の登録に含める登録タイプを一度に 1 つずつ選択し、データを入力します。 • [トラップ（Trap）]：トラップ サブスクリプション タイプのフィールドにデータを入力します。 • [E-Mail]：[E-Mail Subscription Type] フィールドにデータを入力します。 • [Syslog（Syslog）]：Syslog サブスクリプション タイプのフィールドにデータを入力します。 Cisco Prime Collaboration Assurance では、[サブスクリプション: 概要（Subscription: Summary）] ページの [完了（Finish）] をクリックするまで、入力したデータが保存されません。[サブスクリプション: 概要（Subscription: Summary）] ページに移動するには、[次へ（Next）] をクリックします。
[Trap Subscription Type] フィールド	
[IP Address/Fully Qualified Domain Name] 編集可能カラム	ホストの IP アドレスまたは完全修飾ドメイン名（FQDN）を入力します。
[Port] 編集可能カラム	ホストがトラップを受信できるポート番号を入力します。有効なポートの値は、0 ～ 65,535 です。デフォルトのポート番号 162 を入力することもできます。
[Comments] 編集可能カラム	（任意）コメントを入力します。
[E-Mail Subscription Type] フィールド	

グラフィカルユーザインターフェイスの要素	説明
[SMTP Server] フィールド	Simple Mail Transfer Protocol（SMTP）サーバの完全修飾 DNS 名または IP アドレスを入力します（デフォルトの SMTP サーバの名前がすでに表示されている場合もあります）。 既存の登録によって使用されているデフォルト以外の任意のSMTPサーバを選択するには、SMTP Servers ボタンをクリックします。 デフォルトの SMTP サーバの設定方法については、「システム環境設定を使用してシステム全体のパラメータを設定する」を参照してください。
[Sender Address] フィールド	通知の送信元の電子メール アドレスを入力します。送信者の電子メール サービスが指定した SMTP サーバでホスティングされている場合は、ユーザ名だけを入力します。ドメイン名を入力する必要はありません。
[Recipient Address(es)] フィールド	通知の送信先となる 1 つ以上の電子メール アドレスを入力します。複数のアドレスはカンマまたはセミコロンで区切ります。 受信者の電子メールサービスが指定したSMTPサーバでホスティングされている場合は、ユーザ名だけを入力します。ドメイン名を入力する必要はありません。
[Send Recipient(s) Subject Only] チェックボックス	電子メール メッセージにサブジェクトだけを含める場合はオンにします。 詳細な電子メール メッセージを送信する場合はオフにします（デフォルト）。 **Cisco Prime Collaboration リリース 11.1 以降の場合** （注） 件名を含む電子メール通知は、次の形式で送信されます。
[PC-ALERT-CLUSTERNAME] DEVICE IP : EVENTNAME : SEVERITY. 例： *[PC-ALERT-CPCM-Ent-Cluster]50.0.50.230:Gatekeeper Registration Failure:CRITICAL* *CLUSTERNAME* は、Unified Communications Manager と Cisco VCS のみの件名の欄に含まれています。他のすべてのデバイス タイプで、*CLUSTERNAME* は空のままになります。 *DEVICE IP* または *CLUSTERNAME* が利用できない場合は、空のままになります。	

グラフィカルユーザインターフェイスの要素	説明
[Syslog Subscription Type] フィールド	
[IP Address/Fully Qualified Domain Name] 編集可能カラム	ホストの IP アドレスまたは完全修飾ドメイン名（FQDN）を入力します。
[Port] 編集可能カラム	syslog デーモンがリスニングを行うポート番号を入力します。有効なポートの値は、0 ～ 65,535 です。デフォルトのポート番号 514 を入力することもできます。 リモート システム（ホスト名）の syslog デーモンが指定したポートでリスニングを行うように設定しておく必要があります。
[Comments] 編集可能カラム	（任意）コメントを含めます。



第 17 章

しきい値ルールの設定

このセクションでは、次の点について説明します。

- しきい値ルールの設定 （267 ページ）
- しきい値ルール （267 ページ）
- TelePresence エンドポイント しきい値の設定—デバイス レベル （270 ページ）
- TelePresence エンドポイント しきい値の設定—グローバル （271 ページ）
- 会議のトラブルシュートに使用するしきい値の設定 （272 ページ）
- TelePresence エンドポイントの自動トラブルシューティングを有効化する （273 ページ）
- デバイス プールのしきい値の概要 （273 ページ）
- デバイス プールしきい値の編集 （275 ページ）
- 音声通話グレード設定の概要 （276 ページ）
- Dynamic Syslog の追加 （276 ページ）
- 相関ルール （279 ページ）
- カスタム アラートの作成 （283 ページ）
- System （286 ページ）

しきい値ルールの設定

このセクションでは、ビジネス ニーズに合わせてアラームやイベントをカスタマイズする方法について説明します。

しきい値ルール

特定のパラメータが事前に定義されたしきい値を超えた場合、イベントを生成するようにデバイスを設定できます。

Cisco Prime Collaboration リリース 11.5 以降の場合

次で設定を実行できます。**[アラームおよびレポートの管理（Alarm & Report Administration）]** > **[イベントのカスタマイズ（Event Customization）]** > **[しきい値ルール（Threshold Rules）]**。

しきい値ルールのページには、[Basic] と [Advanced] の 2 つのタブがあります。[Basic] タブには、Cisco Prime Collaboration Assurance で生成または抑制できるインライン イベントが一覧表示されています。

[Advanced] タブには有効なイベントがすべて表示され、ユーザはカスタム イベントを作成することもできます。カスタム イベントを作成するには **[Add Event]** をクリックし、ドロップダウンからクラスタまたはデバイスを選択し、必要な詳細情報を入力して **[Save]** をクリックします。

Cisco Prime Collaboration リリース 11.1 以降の場合

これらの両方のタブに表示される各イベントに対して、イベントを展開して **[Custom Rule]** をクリックすると、カスタムのしきい値を追加または編集することができます。[Basic] タブでは、選択したデバイス タイプに基づきしきい値のみを作成できますが、[Advanced] タブでは、アラートのスケジューリング、設定の頻度、重大度など、作成したしきい値にルールを設定することもできます。カスタムのしきい値ルールはデバイス レベルまたはデバイス タイプ レベルで追加、編集、削除できます。すべてのデバイスに適用する変更の場合は、[Apply for All Devices] チェックボックスをオンにしてください。

[Basic] タブおよび [Advanced] タブの両方で、**[電子メールのメモ（Notes for Email）]** 用のイベントに関する追加情報を追加でき、メモは 1000 文字以内で作成します。また、[編集（Edit）] や [削除（Delete）] のリンクを使用して、[電子メールのメモ（Notes for Email）] を編集または削除することもできます。メモを編集する場合は、少なくとも 1 文字を [電子メール用メモ（Notes for Email）] に残しておきます。この追加情報は、通知として電子メールで送信されます。

ドル（$）、縦線（|）、チルダ（~）などの特殊文字を **[電子メールのメモ（Notes for Email）]** に追加することは推奨されていません。

[Advanced] タブで **[Custom Rule]** をクリックすると、[Add Alert Settings] ページが表示されます。**[デバイス タイプ（Device Type）]**、**[クラスタ（Cluster）]** を選択して **[次へ（Next）]** をクリックします。[Add Threshold Rules] タブに必要な詳細情報を入力して **[Save]** をクリックします。

イベントとしきい値の追加だけではなく、次の表に記載されている処理も実行できます。

アクション	Basic	Advanced

重大度の変更	はい 名前のチェックボックスをオンにする—すべてのイベントを選択するか、選択するイベントのチェックボックスをオンにして、**[重大度の変更（Change Severity）]** をクリックします。	はい 名前のチェックボックスをオンにする—すべてのイベントを選択するか、選択するイベントのチェックボックスをオンにして、**[重大度の変更（Change Severity）]** をクリックします。 [Custom Rule] オプションを使用してカスタムしきい値の重大度を変更することも、[Edit Threshold] オプションを使用してカスタム イベントの重大度を変更することもできます。
イベントの生成または抑制	はい 名前のチェックボックスをオンにする—すべてのイベントを選択するか、選択するイベントのチェックボックスをオンにして、**[生成（Raise）]** または **[抑制（Suppress）]** をクリックします。	はい 名前のチェックボックスをオンにする—すべてのイベントを選択するか、選択するイベントのチェックボックスをオンにして、**[生成（Raise）]** または **[抑制（Suppress）]** をクリックします。
しきい値の生成または抑制	はい イベントを展開してしきい値を選択し、ドロップダウンから **[生成（Raise）]** または **[抑制（Suppress）]** を選択します。	はい イベントを展開してしきい値を選択し、ドロップダウンから **[生成（Raise）]**、**[抑制（Suppress）]**、または **[条件付き（Conditional）]** を選択します。
既存のしきい値の編集、リセット、および削除	いいえ しきい値の設定は編集またはリセットできますが、削除はできません。 しきい値を編集またはリセットするには、イベントを展開してしきい値の設定を編集し、**[Save Changes]** をクリックします。	はい しきい値を編集またはリセットするには、イベントを展開してしきい値の設定を編集し、**[Save Changes]** をクリックします。 削除できるのはカスタムのしきい値のみです。しきい値を削除するには、イベントを展開して、しきい値を選択し、**[Delete]** をクリックします。

イベントの編集または削除	いいえ	はい イベントを展開し、設定を編集して **[Save]** をクリックします。 削除できるのはカスタム イベントのみです。イベントを削除するには、チェックボックスをオンにして **[Delete]** をクリックします。
イベントの複製	いいえ	はい **[クローン（Clone）]** をクリックして詳細を入力し、**[保存（Save）]** をクリックします。 （注） 複製オプションは、CVP および Unified CCE デバイスに対してのみ使用できます。このオプションは、Communication Manager、Media Sense、IM and Presence、Finesse などの他のデバイス タイプのイベントについては無効です。

TelePresence エンドポイント しきい値の設定—デバイス レベル

Cisco Prime Collaboration リリース 11.5 以前の場合

しきい値をグローバル レベルで適用しない場合は、次の手順を実行して、デバイス レベルで Cisco TelePresence エンドポイントのしきい値を設定します。

ステップ 1 選択 **[アシュアランス管理（Assurance Administration）]** > **[イベントのカスタマイズ（Event Customization）]** > **[しきい値ルール（Threshold Rules）]**。

Cisco Prime Collaboration リリース 11.5 以降の場合

移行方法 **[アラームおよびレポートの管理（Alarm & Report Administration）]** > **[イベントのカスタマイズ（Event Customization）]** > **[しきい値ルール（Threshold Rules）]** 。

ステップ 2 [基本（Basic）] タブで、[ジッター（Jitter）]、[パケット損失（Packet loss）]、[遅延イベント（Latency event）] を展開し、しきい値を [やや重大（Minor）]、[重大（Major）]、[深刻（Critical）] に変更します。

イベントを発生させる、または抑制するオプションもあります。

ステップ 3 **[保存の変更（Save Changes）]** をクリックします。

あるデバイス タイプのすべてのデバイスに変更を適用することも、選択したデバイスに変更を適用することもできます。これを行うには、[カスタムルール（Custom Rule）] をクリックして、デバイス タイプを選択します。すべてのデバイスに適用するには、この [タイプ（Type）] の [すべてのデバイス（All Devices）] を選択します。選択したデバイスに変更を適用するには、[デバイスの選択（Select Devices）] をクリックし、選択するデバイスを選び [保存（Save）] をクリックします。

デバイスを検索するには、[表示（Show）] ドロップダウン リストから [簡易フィルタ（Quick Filter）] を選択し、そのデバイスのホスト名または IP アドレスを入力します。

TelePresence エンドポイント しきい値の設定—グローバル

Cisco Prime Collaboration リリース 11.1 以前の場合

しきい値がすべての TelePresence デバイスの Rx パケット損失、ジッター、遅延用に設定された制限を超える場合にように、Cisco Prime Collaboration Assurance を設定できます。

TelePresence エンドポイントのしきい値を設定するには、次の手順を実行します。

ステップ 1 選択 **[アシュアランス管理（Assurance Administration）]** > **[会議パスのしきい値設定（Conference Path Threshold Settings）]**。

ステップ 2 [Rxパケット損失（Rx Packet Loss）]、[平均期間のジッター（Average Period Jitter）]、[DSCP] の値を変更し、[保存（Save）] をクリックします。

しきい値のポーリング間隔を変更することもできます。値をデフォルトにリセットする場合は、[デフォルトにリセット（Reset to Default）] をクリックします。

TelePresence しきい値が定義された値を超える場合、自動トラブルシューティングの開始を有効にすることができます。次に進む: **[アシュアランス管理（Assurance Administration）]** > **[イベントのカスタマイズ（Event Customization）]** > **[しきい値ルール（Threshold Rules）]**[基本（Basic）] タブで、[ジッター（Jitter）]、[パケット損失（Packet loss）]、[遅延イベント（Latency event）] を展開し、[自動トラブルシューティング（Automatic Troubleshooting）] ドロップダウン リストから [やや重大（Minor）]、[重大（Major）]、

[深刻（Critical）] を選択します。無効にするには、ドロップダウン リストから [無効（Disabled）] を選択します。

次のタスク

Cisco TelePresence エンドポイントをデバイス レベルで設定する方法の詳細については、『Cisco Prime Collaboration Assurance ガイド - Advanced, 11.x』の「「TelePresence エンドポイントのしきい値の設定：デバイス レベル」」セクションを参照してください。

会議のトラブルシュートに使用するしきい値の設定

Cisco Prime Collaboration リリース 11.6 以降の場合

Cisco Prime Collaboration Assurance でしきい値を設定すると、パス内のメトリック違反を表示したり、すべての TelePresence デバイスに対し、しきい値が Rx パケット損失、ジッター、または遅延に対して設定された制限を超えた場合に自動トラブルシューティングを開始したりできます。

TelePresence エンドポイントのしきい値を設定するには、次の手順を実行します。

ステップ 1 選択 **[アラームおよびレポート管理（Alarm & Report Administration）]** > **[会議パスのしきい値設定（Conference Path Threshold Settings）]**。
[会議パスのしきい値設定（Conference Path Threshold Settings）] ページが表示されます。

ステップ 2 パス統計の吹き出しの色を変更する場合は、[メモリ使用率（Memory Utilization）] と [Rxパケット損失（Rx Packet Loss）] の値を変更します。

また、パス内の任意のメトリック違反について、[CPU使用率（CPU Utilization）]、[平均期間のジッター（Average Period Jitter）]、および [DSCP（DSCP）] の値を変更することもできます。すべてのデバイスに対し、しきい値が [Rxパケット損失（Rx Packet Loss）]、[平均期間のジッター（Average Period Jitter）]、または [DSCP（DSCP）] に設定された制限を超えると、青色のバッジ情報アイコンが [パスビュー（Path View）] と [クイックビュー（Quick View）] に表示されます。

ステップ 3 （省略可）ポーリング間隔を変更する場合は、[フロー統計のポーリング間隔（Statistics Polling Interval）] の値を変更します。

ステップ 4 **[保存（Save）]** をクリックします。

値をデフォルトにリセットする場合は、[デフォルトにリセット（Reset to Default）] をクリックします。

TelePresence エンドポイントの自動トラブルシューティングを有効化する

Cisco Prime Collaboration リリース 11.6 以降の場合

次の手順を実行して、しきい値がパケット損失、ジッター、遅延に定義された値を超える場合に会議の自動トラブルシューティングを有効にします。

手順の概要

1. 選択 **[アラーム & レポート管理（Alarm & Report Administration）]** > **[Event Customization（イベントのカスタマイズ）]** > **[しきい値ルール（Threshold Rules）]**。
2. [基本（Basic）] タブで、[ジッター（Jitter）]、[パケット損失（Packet loss）]、[遅延イベント（Latency event）] を展開し、[自動トラブルシューティング（Automatic Troubleshooting）] ドロップダウン リストから [やや重大（Minor）]、[重大（Major）]、[深刻（Critical）] を選択します。

手順の詳細

ステップ 1 選択 **[アラーム & レポート管理（Alarm & Report Administration）]** > **[Event Customization（イベントのカスタマイズ）]** > **[しきい値ルール（Threshold Rules）]**。

ステップ 2 [基本（Basic）] タブで、[ジッター（Jitter）]、[パケット損失（Packet loss）]、[遅延イベント（Latency event）] を展開し、[自動トラブルシューティング（Automatic Troubleshooting）] ドロップダウン リストから [やや重大（Minor）]、[重大（Major）]、[深刻（Critical）] を選択します。

無効にするには、ドロップダウン リストから**[無効（Disabled）]** を選択します。

デバイス プールのしきい値の概要

デバイス プールは、デバイスの論理グループです。デバイス プールは、たとえばデバイスが配置される領域など、デバイスに割り当てることができる一連の共通した性質を定義する便利な方法を提供します。

Cisco Prime Collaboration Assurance 内では、デバイス プールはクラスタ検出の完了後のみに表示されます。しきい値ウィンドウにデバイス プールが 1 つも表示されない場合は、実行するインベントリをスケジュールします。デフォルトでは、クラスタ デバイス検出はスケジュールされていません。

（注） デバイス プールに接続するデバイスがない場合、Cisco Prime Collaboration Assurance は、クラスタ デバイス検出が完了したとしても、デバイス プールを表示されません。

でのデバイス プールのしきい値設定により、ユーザが集約イベントの量を設定できます。

- デバイスプールのしきい値のいずれかのパーセンテージでの設定をデフォルト設定または現在の設定から上げると、受け取る集約イベントの量が減ります。
- デバイスプールのしきい値のパーセンテージでの設定をデフォルト設定または現在の設定から下げると、そのデバイスプールからより多くの集約イベントを受け取ることになります。

影響を受けた電話機の数がしきい値と同じである場合、Cisco Prime Collaboration Assurance は、1 つのサービス品質イベントを発生させます。

たとえば、デバイス プールに 100 台の電話が含まれており、10 台の電話がネットワークの問題による影響を受けたとすると、デバイス プールのしきい値が 10% の場合に、このデバイス プールについて 1 つの集約イベントを受け取ることになります。

集約イベントが 1 つ発生した後は、そのイベントがクリアされるまで別の集約イベントは一切送信されません。集約イベントをクリアするには、まず個々のデバイスイベントまたはサービス品質イベントをすべてクリアする必要があります。

（注） "ServiceQualityThresholdCrossed" イベントの場合、Cisco Prime Collaboration Assurance は しきい値を少数から整数へと四捨五入します。

Cisco Prime Collaboration リリース 11.6 の場合

（注） "ServiceQualityThresholdCrossed" と "PhoneUnregThresholdExceeded" イベントの場合、Cisco Prime Collaboration Assurance はしきい値を少数から整数へと四捨五入します。

Cisco Prime Collaboration Assurance を MSP モードで導入した場合、表示されたデバイス プールは、グローバル [顧客選択（Customer Selection）] フィールドで選択したお客様に属します。

Cisco Prime Collaboration リリース 12.1 以降の場合

（注） "ServiceQualityThresholdCrossed" と "EndpointUnregThresholdExceeded" イベントの場合、Cisco Prime Collaboration Assurance はしきい値を少数から整数へと四捨五入します。

Cisco Prime Collaboration Assurance を MSP モードで導入した場合、表示されたデバイス プールは、グローバル [顧客選択（Customer Selection）] フィールドで選択したお客様に属します。

Cisco Prime Collaboration Assurance は、これらのデバイス プールのしきい値イベントを、サービス レベルのイベントではなくデバイス イベントとみなします。

デバイス プールしきい値の編集

Cisco Prime Collaboration Assurance を使用してデバイス プールのしきい値を表示および設定するには、次の手順を実行します。

ステップ 1 選択 **[イベントのカスタマイズ（Event Customization）]** > **[相関ルール（Correlation Rules）]**。

Cisco Prime Collaboration リリース 11.5 以降の場合

移行方法 **[アラームおよびレポートの管理（Alarm & Report Administration）]** > **[イベントのカスタマイズ（Event Customization）]** > **[相関ルール（Correlation Rules）]**。

ステップ 2 EndpointUnregThresholdExceeded または ServiceQualityThresholdCrossed イベントを選択します。

このウィンドウにデバイス プールが 1 つも表示されない場合は、実行するクラスタ インベントリをスケジュールします。

ステップ 3 表示または編集するデバイス プールの横にあるチェックボックスをオンにします。

ステップ 4 [Edit] をクリックします。

ステップ 5 現在のデフォルトのしきい値を編集するには、次の手順を実行します。

a) グループを選択して、デフォルトのしきい値を変更し、[編集（Edit）] をクリックします。

b) [電話登録解除しきい値/サービス品質しきい値（Threshold/Service Quality Threshold）] ダイアログボックスで、しきい値を編集し、[保存（Save）] をクリックします。

すべてのパラメータ タイプを Cisco Prime Collaboration Assurance のデフォルト設定にリセットするには、次の操作を実行します。

c) すべてのデバイス プールまたは CME のチェックボックスをオンにして、**[元に戻す（Revert）]** をクリックします。

d) **[保存（Save）]** をクリックします。

変更がデータベースに保存されます。ただし、まだ IP ファブリックに適用されていません。

このタイプの集約イベントが発生したときに自動的に通知されるようにするには、このイベントが発生したときに電子メールが送信されるように通知を設定します。電子メール通知の設定方法の詳細については、『Cisco Prime Collaboration Assurance ガイド：Advanced』の「通知の設定」を参照してください。

音声通話グレード設定の概要

音声品質の変化は、Severely Conceal Seconds Ratio（SCSR）（%）に基づいて実行されます。これは、MOSベースのグレーディングよりも、通話全体で品質を向上させることができます。また、特に広帯域コーデックなど、さまざまな音声コーデックもサポートしています。MOSからSCSR（%）への移行に関する詳細については、『Cisco Prime Collaboration Assurance および Analytics：VoIP コールの効率性と信頼性のグレードに関するホワイトペーパー』を参照してください。

通話は、通話の長さに基づきロング コールまたはショート コールとして分類されます。通話時間が 20 秒以上のものはロング コール、20 秒未満のものはショート コールとされます。

ロング コール SCSR（%）とショート コール SCSR（%）のしきい値は更新できます。ショートコールSCSR（%）とロングコールSCSR（%）のしきい値設定は異なります。次の表には、利用可能な通話グレードの詳細が示されています。

通話グレード	説明
Poor	通話の SCSR（%）値がロング コール SCSR（%）またはショートコールSCSR（%）のしきい値よりも大きい場合、通話グレードはPoorです。
Acceptable	通話の SCSR（%）値がロングコール SCSR（%）またはショートコールSCSR（%）のしきい値以上の場合、通話グレードはAcceptableです。
Good	通話の SCSR（%）値がロングコール SCSR（%）またはショートコールSCSR（%）のしきい値よりも下回る場合、通話グレードはGood です。

ロングコール SCSR（%）またはショート コール SCSR（%）のしきい値を設定するには、**[アラームおよびレポート管理（Alarm & Report Administration）] > [CDR分析の設定（CDR Analysis Settings）] > [音声コールグレードの設定（Configure Voice Call Grade）]** を選択して、適切なフィールドにしきい値を入力します。しきい値をデフォルト設定に戻すには、**[デフォルトにリセット（Reset to Default）]** をクリックします。

Dynamic Syslog の追加

Cisco Prime Collaboration Assurance では、サポートされていない syslogs を追加できます。Cisco Prime Collaboration Assurance で syslog を使用する前に、デバイスから正確な syslog 詳細を取得する必要があります（たとえば、正確な syslog 名を入力するなど）。入力する syslog 名はイベント名として使用されます。

syslog をクリアする必要がある重大度と時間を設定できます。

（注） Dynamic Syslog は、TP_CONDUCTOR と Cisco 以外のデバイスを除くすべてのデバイスをサポートします。

（注） Syslog 通信は UDP を介してサポートされます。

次のような syslog を追加しないことを推奨します。

- Syslogs は、大量に生成されることがあるため、Cisco Prime Collaboration Assurance 過度の負荷がかかる可能性があります。
- 20 を超える syslog。

Cisco Prime Collaboration リリース 11.1 以降の場合

イベントまたはアラームに関する追加情報を [電子メールのメモ（Notes for Email）] に追加できます。メモは1000 文字以内でなくてはなりません。また、[編集（Edit）]や[削除（Delete）]のリンクを使用して、[電子メールのメモ（Notes for Email）]を編集または削除することもできます。メモを編集する場合は、少なくとも 1 文字を [電子メール用メモ（Notes for Email）] に残しておきます。この追加情報は、通知として電子メールで送信されます。

ドル（$）、縦線（|）、チルダ（~）などの特殊文字を、[電子メールのメモ（Notes for Email）] に追加することは推奨されていません。

syslog を追加するには、次の手順を実行します。

ステップ 1 **[アシュアランス管理（Assurance Administration）] > [イベントのカスタマイズ（Event Customization）] > [Syslog ルール（Syslog Rules）]**。

Cisco Prime Collaboration リリース 11.5 以降の場合

移行方法 **[アラームおよびレポート管理（Alarm & Report Administration）] > [イベントのカスタマイズ（Event Customization）] > [Syslog ルール（Syslog Rules）]**。

ステップ 2 [Add Event] をクリックします。

[新しいSyslogイベント（New Syslog Event）] ウィンドウが開きます。次を入力します。

- Syslog 名
- イベントの説明
- イベントの重大度
- Event Clear Interval

ステップ 3 （任意）[発生ごとにイベントを生成する（Raise Event for Each Occurrence）] チェックボックスをオンにします。

このオプションは慎重に使用してください。Cisco Prime Collaboration Assurance によって、syslog ごとにイベントが生成されます。この場合、syslogs に毎回固有の詳細情報が表示されていれば、これは実現可能な選択肢です。

ステップ 4 **[保存（Save）]** をクリックします。

次の操作を実行できます。

- [編集（Edit）] オプションを使用してイベント名、重大度を変更し、[発生ごとにイベントを生成する（Raise Event for Each Occurrence）] チェックボックスをオンまたはオフにします。
- syslog名またはイベントの重大度をカスタマイズする。これを行うには、[イベントのカスタマイズ（Event Customization）] ページに移動します。詳細については、『Cisco Prime Collaboration Assurance Advanced - ガイド』しきい値ルールの設定 （267 ページ）の

例

以下は、クラスタにバックアップされていない ITLRecovery 証明書がある場合に発生する、サポート対象外の syslog の例です。

次の値を入力します。

- Syslog 名：ITLRecoveryCertBackup
- イベントの説明：ITLRecoveryCertBackup イベント
- イベント重大度：メジャー
- イベントのクリア間隔：1 時間

（注） イベントの重大度とイベントのクリア間隔の値は設定可能です。

<187>9009: Jul 31 2017 16:05:38.777 IST :%UC_CERT-4-ITLRecoveryCertBackup: %[Message=][AppID=Cisco Certificate Monitor][ClusterID=ccm234][NodeID=cucm107886234]：このクラスタには、バックアップされていない ITLRecovery 証明書があります。クラスタ再構成操作の後に、クラスタ内のすべての電話から ITL ファイルを手動で削除する必要がないように、この証明書の手動バックアップを取ることを推奨します。

相関ルール

接続されているデバイスからイベントが発生すると、Cisco Prime Collaboration Assurance は相関ルールを適用します。次の表では、あるデバイスが、指定された時間枠内の特定の頻度でイベント A とイベント B（または単一イベント）を発生させた場合に、Cisco Prime Collaboration Assurance がこれらのイベントを相互に関連付け、アラームを生成することについて説明しています。アラームは 24 時間以内に自動でクリアされます。

たとえば、使用率のしきい値が変更されるたびに、Cisco Prime Collaboration Assurance は High Utilization イベントを生成します。高使用率イベントが 20 分間の間に 2 度発生した場合、High Utilization Detected アラームが発生します。

次に、Cisco Prime Collaboration Assurance の定義済みの相関ルールを示します。

Cisco Prime Collaboration Contact Center Assurance ライセンスを追加すると、特定の相関ルールを、Cisco Prime Collaboration Contact Center Assurance に対して排他的に適用できます。詳細については、『Cisco Prime Collaboration Contact Center Assurance ガイド』の 「「Contact Center の相関ルール」」のセクションを参照してください。

相関ルールの名前	アラームを発生させる主なイベント	主なイベントが原因で発生する現象イベント	相関アラームの名前	相関アラームが発生するタイミング	主なイベントと現象イベントを受信する（最小）時間枠	発生回数
Call Throttling Detected	Code Yellow、CpuPegging	NA	CodeYellow	両方のメインイベントが発生する。	20	1
Interface Flapping	OperationallyDown、OperationallyDown cleared	NA	Interface Flapping	Operationis Down が 3 インスタンス以上の場合は、OperationallyDown cleared イベントが代わりに発生します。	20	3

相関ルールの名前	アラームを発生させる主なイベント	主なイベントが原因で発生する現象イベント	相関アラームの名前	相関アラームが発生するタイミング	主なイベントと現象イベントを受信する（最小）時間枠	発生回数
Repeated Location Bandwidth Out Of Resource	LocationBWOutOfリソース	NA	Repeated Location Bandwidth Out Of Resource	LocationBWs-OutOfResourceが、3インスタンス以上の場合に Cisco Unified Communications Manager で発生します。	20	3
WAN Link Outage Detected	Unresponsive	NA	Wan Link Outage Detected	Unresponsive イベントがトリガーされた場合。	10	NA
（注） このルールは、ユーザインターフェイスから編集したり削除したりすることはできません。						
VM Down	VMDown	Unreachable	VMDown	ICMP ポーリングに基づき、VMDown トラップを vCenter から受信し、VMに対する Unreachable イベントを受信した場合。	5	NA

相関ルールの名前	アラームを発生させる主なイベント	主なイベントが原因で発生する現象イベント	相関アラームの名前	相関アラームが発生するタイミング	主なイベントと現象イベントを受信する（最小）時間枠	発生回数
ESX Host Down	HostConnection Failure	Unreachable、VMDown	ESXHost ダウン	HostConnection Failure トラップを vCenter から受信し、ICMP ポーリングに基づき、ESXHost に対する Unreachable イベントを受信した場合。	5	NA
Network Down	NetworkConnectivity Lost、LostNetwork Connectivity ToDVPorts	Unreachable	ネットワーク ダウン	ICMP ポーリングに基づき、主なイベントのいずれかが発生し、ESXHost に対する Unreachable イベントを受信した場合。	5	NA
UCS Chassis Down	ChassisInOperable、ChassisIOCardInaccessible、ChassisThermal ThresholdNon Recoverable	Unreachable、VMDown、HostConnection Failure、ネットワーク ConnectivityLost	UCS シャーシ ダウン	主なイベントの 1 つが発生した場合。	5	NA

相関ルールの名前	アラームを発生させる主なイベント	主なイベントが原因で発生する現象イベント	相関アラームの名前	相関アラームが発生するタイミング	主なイベントと現象イベントを受信する（最小）時間枠	発生回数
エンドポイント Unreg しきい値（Threshold）Exceeded	該当なし	該当なし	エンドポイント Unreg しきい値（Threshold）Exceeded	該当なし	該当なし	該当なし
電話未登録しきい値（Threshold）Exceeded			電話未登録しきい値（Threshold）Exceeded			
サービス品質しきい値（Threshold）Crossed	該当なし	該当なし	サービス品質しきい値（Threshold）Crossed	該当なし	該当なし	該当なし

[イベントのカスタマイズ（Event Customization）] ページの上部で、使用可能な検索オプションを使用してイベントを検索してフィルタすることができます。ただし、[関連付けルール（Correlation Rules）] の下にリストされているイベントについては、イベントの名前が一意ではなく、[イベントのカスタマイズ（Event Customization）] ページの他のタブにリストされたイベントと名前が同じ場合に、名前ベースの検索が機能しません。[相関ルール（Correlation Rules）] タブでイベントを検索するには、相関ルールの名前を使用します。

Cisco Prime Collaboration リリース 11.1 以降の場合

イベントまたはアラームに関する追加情報を **[電子メールのメモ（Notes for Email）]** に追加できます。メモは1000文字以内でなくてはなりません。また、[編集（Edit）]や[削除（Delete）] のリンクを使用して、[電子メールのメモ（Notes for Email）] を編集または削除することもで

きます。メモを編集する場合は、少なくとも 1 文字を [電子メール用メモ（Notes for Email）] に残しておきます。この追加情報は、通知として電子メールで送信されます。

ドル（$）、縦線（|）、チルダ（~）などの特殊文字を [電子メールのメモ（Notes for Email）] に追加することは推奨されていません。

Cisco Prime Collaboration Assurance のすべての相関ルールで、アラーム抑制ロジックがデフォルトで適用されます。指定された時間枠内でイベント A またはイベント B が発生した場合、最初に、相関アラームが対応するイベントと共にトリガーされます。個々のイベントのアラームは、相関の条件を満たさないまま指定された時間枠が経過した後にのみ発生します。たとえば、ロガー、PG、またはルータなどの Unified CCE コンポーネントがダウンすると、Cisco Prime Collaboration Assurance は、相関アラームと一連のイベントを生成します。イベントのアラームは、10 分の時間間隔を過ぎても相関が起きなかった場合にのみ発生します。アラーム抑制を無効にするには、相関ルールを選択して [編集（Edit）] をクリックします。[相関ルールの編集（Edit Correlation Rule）] ページで、[アラーム抑制を無効にする（Disable Alarm Suppression）] チェックボックスをオンにし、[保存（Save）] をクリックします。

（注） 相関ルールに対してアラーム抑制ロジックを無効にしても、その相関ルールのイベントの部分を生成できないわけではありません。イベントが 2 つ以上の相関ルールに含まれ、かつアラーム抑制ロジックがそのいずれかのルールに適用されている場合は、もう一方のルールが優先されてイベントが発生する可能性があります。

VMware vCenter Server のアラームのトリガー：VMware vCenter Server（vCenter）のトリガーを無効化または変更すると、vCenter アラームの生成がブロックされるので避けてください。これらのトリガーのリストについては、Cisco Prime Collaboration Assurance 11.0 の場合は『Setting Up Devices for Cisco Prime Collaboration Assurance 11.0 Wiki ページ』を、Cisco Prime Collaboration Assurance 11.5 の場合は『Prime Collaboration Assurance 11.5 のデバイス設定』を参照してください。VMware vCenter Server のイベントとアラームのリストを表示するには、『Cisco Prime Collaboration でサポートされているアラームとイベント』を参照してください。VMware vCenter Server（vCenter）の詳細については、『vSphere - ESX and VCenter Datacenter 管理者ガイド』を参照してください。

カスタム アラートの作成

カスタム アラートを作成できます。しきい値およびアラート トリガー パラメータを含めることもできます。パラメータの詳細については、「カスタムアラートのパラメータ」を参照してください。

カスタム アラートを作成するには

ステップ 1　Cisco Prime Collaboration リリース 11.5 以降の場合

移行方法 **[アラームおよびレポートの管理（Alarm & Report Administration）] > [イベントのカスタマイズ（Event Customization）] > [しきい値ルール（Threshold Rules）]**。

また、作成したカスタム ダッシュボードからイベントを直接追加することもできます。

ステップ 2 [Add Event] をクリックします。

ステップ 3 [New Performance Counter Event] ページで、以下を実行します。

a) クラスタおよびサーバを指定します。

b) [Available Counters] ドロップダウン リストからカウンタを選択します。

Cisco Prime Collaboration Assuran を MSP モードでインストールした場合は、サーバとカウンタを選択すると、パブリック IP アドレスが表示されます。ただし、特定のパフォーマンス カウンタまたはデバイスが Cisco Prime Collaboration Assurance で追加または管理されていない場合は、これらのノードのカスタム イベントを作成したり追加したりすることはできません。

また、[Cluster] ドロップダウン リストには、（グローバル フィルタのドロップダウンから選択された）特定のカスタマーに属している製品とクラスタのみが表示されます。

c) 説明と推奨処置を追加します。これは任意です。

d) モニタリングのしきい値、持続時間および頻度、ならびにスケジュールを指定します。

e) **[Save]** をクリックします。

（注） デバイス上のパフォーマンス カウンタに対して作成されたしきい値ルールは、データベースに保存されます。これにより、カウンタの値が、しきい値ルールで定義されたしきい値の条件に違反した場合にアラームが生成されます。パージ ポリシーの詳細については、『Cisco Prime Collaboration Assurance ガイド—Advanced』の「パージ ポリシー」の章を参照してください。

カスタム アラートのパラメータ

ユーザがカスタム アラートに指定できるパラメータを表に示します。

設定	説明
しきい値	
	チェックボックスをオンにして適用する値を入力します。 • [Over]：このチェックボックスをオンにして、アラート通知がアクティブになる前に一致する必要がある最大しきい値を設定します。[以上（Over）] の値フィールドには、値を入力します。たとえば、進行中のコールの数と等しい値を入力します。 • [Under]：このチェックボックスをオンにして、アラート通知がアクティブになる前に一致する必要がある最小しきい値を設定します。[以下（Under）] の値フィールドには、値を入力します。たとえば、進行中のコールの数と等しい値を入力します。 （注） これらのチェックボックスは、[頻度（Frequency）] および [スケジュール（Schedule）] の設定パラメータと組み合わせて使用します。

設定	説明
値	
	適用するオプション ボタンをクリックします。 • [Absolute]：データの現在の状態を表示する場合に選択します。これらのカウンタ値は累積されます。 • [Delta]：現在のカウンタ値と前回のカウンタ値の差分を表示する場合に選択します。 • [Delta Percentage]：カウンタ パフォーマンスの変化を比率で表示する場合に選択します。
持続時間	
• Trigger alert only when value constantly... • Trigger immediately	• [Trigger alert only when value constantly...]：指定時間（秒）内に値が常にしきい値の下限または上限を超える場合に限りアラート通知を送信する場合、このオプション ボタンをクリックして、アラートを送信するまでの指定秒数を入力します。 • [Trigger immediately]：アラート通知をすぐに送信する場合は、このオプション ボタンをクリックします。
頻度	
• Trigger on every poll • Trigger <> events within <> minutes	適用するオプション ボタンをクリックします。 • [Trigger on every poll]：各ポーリングでしきい値条件が一致したときにアラート通知をアクティブにする場合は、このオプション ボタンをクリックします。 たとえば、進行中のコールが継続的にしきい値の上限または下限を超える場合、システムは別のアラート通知を送信しません。しきい値が通常の値（進行中のコール数が 50 ～ 100）の場合、システムはアラート通知を非アクティブにしますが、値がしきい値の上限または下限を再び超えた場合、システムはアラート通知を再びアクティブにします。 • [Trigger <> events within <> minutes]：特定の間隔でアラート通知をアクティブにする場合は、このオプション ボタンをクリックし、送信するアラートと、何分以内に送信するかを入力します。
スケジュール	

設定	説明
• Trigger immediately (Non-stop monitoring) • Schedule between <> to <>	適用するオプション ボタンをクリックします。 • [Trigger immediately (Non-stop monitoring)]：アラートを 1 日 24 時間送信する場合は、このオプション ボタンをクリックします。 • [Schedule between <> to <>]：アラート通知を特定のタイム フレームでアクティブにする場合は、このオプションボタンをクリックし、開始時刻と停止時刻を入力します。このチェックボックスがオンになっている場合は、日次タスクの開始時間と停止時間を入力します。たとえば、カウンタを毎日午前 9 時から午後 5 時まで、または午後 9 時から午前 9 時までチェックするように設定することができます。

System

Cisco Prime Collaboration リリース 11.1 以降の場合

および

Cisco Prime Collaboration リリース 11.5 以降の場合

Cisco Prime Collaboration Assurance の事前定義されたすべてのアラームとイベントを次の通り表示できます。**[アラームおよびレポートの管理（Alarm & Report Administration）] > [イベントのカスタマイズ（Event Customization）] > [システム（System）]**。

システムタブには、次の情報が表示されます。

- 名前
- カテゴリ
- ステータス
- 重大度
- デフォルトの重大度
- **Cisco Prime Collaboration リリース 11.1 以降の場合**

  シスコの規則
- **Cisco Prime Collaboration リリース 11.5 以降の場合**

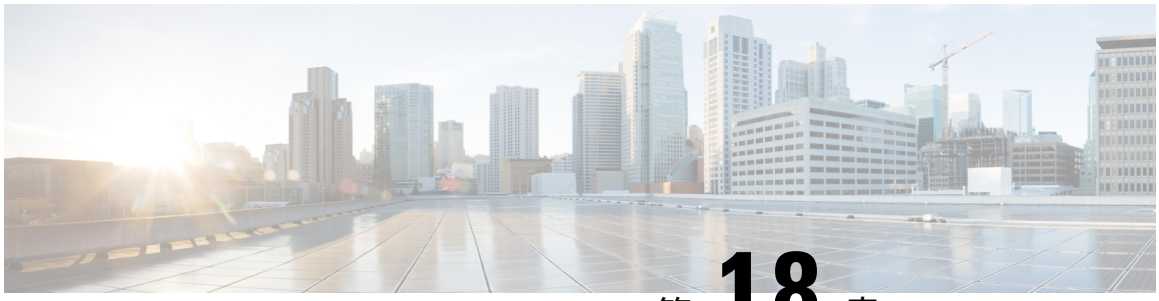
  例外インジケータ
- 電子メール用のメモ

（注） イベントまたはアラームに関する追加情報を **[電子メールのメモ（Notes for Email）]** に追加できます。メモは1000文字以内でなくてはなりません。また、[編集（Edit）]や[削除（Delete）]のリンクを使用して、[電子メールのメモ（Notes for Email）] を編集または削除することもできます。メモを編集する場合は、少なくとも 1 文字を [電子メール用メモ（Notes for Email）] に残しておきます。この追加情報は、通知として電子メールで送信されます。

ドル（$）、縦線（|）、チルダ（~）などの特殊文字を [電子メールのメモ（Notes for Email）] に追加することは推奨されていません。

次の操作を実行できます。

アクション	説明
重大度の変更	名前のチェックボックスをオンにする：すべてのイベントを選択するか、選択するイベントのチェックボックスをオンにして、[重大度の変更（Change Severity）] をクリックします。
イベントの生成または抑制	名前のチェックボックスをオンにする：すべてのイベントを選択するか、選択するイベントのチェックボックスをオンにして、[生成（Raise）]または[抑制（Suppress）]をクリックします。



第 18 章

アラームとイベントのモニタリング

このセクションでは、次の点について説明します。

• アラームとイベントのモニタリング （289 ページ）

アラームとイベントのモニタリング

この章では、アラームとイベントのモニタリングについて説明します。

アラームおよびアラーム サマリー

[Alarms] ページと [Alarm Summary] ページを表示することができます。 **[モニタ（Monitor）]** > **[アラーム & イベント（Alarms & Events）]**。

[Alarms] タブには、Alarm ブラウザの各アラームの次の情報が表示されます。

Severity

アラームの重大度が表示されます。アラームの重大度は、「重大」、「やや重大」、「軽度」、「警告」のいずれかです。アラームの折りたたみアイコンには、アラームの一般情報、メッセージ、コメント、アラームに対する推奨処置が表示されます。

アラームに関連付けられているイベントを表示するには、アラームの重大度にマウスを合わせてクイック ビューアイコンをクリックします。[Events for Alarm] ページが表示され、次の詳細が示されます。

- [説明（Description）]：アラームの説明。
- [ステータス（Status）]：アラームをトリガーしたデバイス。
- [時刻（Time）]：アラームが発生した日付と時刻。

このサマリー ウィンドウは、最新の 5 つのイベントのみがリストされます。すべてを網羅したリストを確認する場合は、[See Event History] を確認してください。

[Events for Alarm] で、次の項目をクリックできます。

- [See Event History] リンク：選択したアラームに関連するイベントを表示します。

- [エンドポイントのモニタ（Monitor Endpoint）] または **[会議のモニタ（Monitor Conference）]** リンクは、[エンドポイントモニタリング（Endpoints Monitoring）] または **[会議モニタリング（Conference Monitoring）]** ページを開きます。このリンクは、会議アラームおよびエンドポイント アラームでのみ表示されます。

クリップボード アイコン/注釈付き

アラームにユーザの注釈が付いていることを示します。

ステータス

アラームのステータスが表示されます。

アラームのクリア状態の詳細を示します。

アラーム名

生成されたアラームの名前。アラーム名、および表示される [Quickview] アイコンにマウスを合わせて、選択したアラームの詳細を表示します。

顧客

Cisco Prime Collaboration Assurance が MSP モードでインストールされている場合は、[アラーム（Alarms）] と [アラームの概要（Alarm Summary）] の両方で、デバイスの所属先であるユーザが表示されます。

デバイス名

アラームがトリガーされたデバイスの名前を表示します。

デバイス IP

デバイスの IP アドレスを表示します。このリンクを使用して、ページ内にエンドポイントまたはインフラストラクチャ デバイス ログを起動することができます。

Cisco Prime Collaboration Assurance が MSP モードで展開されている場合は、このリンクを使用してページ内にエンドポイントまたはインフラストラクチャ デバイス ログを開くことはできません。

コンポーネント名

デバイス名、またはデバイス プール、インターフェイスなどのコンポーネントの名前。

最終更新日

アラームの発生日時を表示します。

デバイス タイプ

デバイスのタイプを表示します。

オーナー

このアラームが割り当てられた人物の名前を表示します。（名前が入力されている場合）。

説明

アラームに関する簡単な説明を表示します。

カテゴリ

アラームのカテゴリを表示します。たとえば、会議、エンドポイント、サービスインフラストラクチャがあります。

エンドポイント名

識別しやすくするためにエンドポイントに割り当てられた名前です。デフォルトでは、[Endpoints Name] 列は非表示になっています。すべての列を表示するには、右上の隅にある [Settings] オプションをクリックします。

モデル

ciscoEX90、ciscoCTS500、ciscoC20 などのデバイス モデルを表示します。

プライベート IP アドレス

Cisco Prime Collaboration Assurance が MSP モードでインストールされている場合は、デバイスのプライベート IP アドレスが表示されます。デフォルトでは、[Private IP Address] 列は非表示になっています。すべての列を表示するには、右上の隅にある [Settings] オプションをクリックします。

アラーム ブラウザを使用することで、次のことができます。

- アラームに関連付けられているイベントの表示：アラーム ステータスの隣のアイコンにマウスを合わせるとポップアップ ウィンドウが表示され、そのアラームに関するすべてのイベントが示されます。
- アラームをクリアするか、確認応答します。
- アラームの割り当て：目的のチェックボックスをオンにし、[assign] ドロップダウン リストの [Assign to me] をクリックします。
- 注釈の追加：目的のチェックボックスをオンにし、[注釈（Annotate）] ドロップダウン リストをクリックして、注釈を追加します。
- アラームの削除：目的のチェックボックスをオンにし、[削除（Delete）] をクリックします。
- 電子メール通知の設定：目的のチェックボックスをオンにし、[電子メール通知（Email Notification）] をクリックします。受信者アドレス、コメント、および件名を入力し、[Submit] をクリックします。サポートされているアラームとイベントの一覧については、『Cisco Prime Collaboration でサポートされているアラームとイベント』を参照してください。

アラームの概要

[アラームの概要（Alarm Summary）] には、各デバイスのアラームのサマリーが表示されます。

次の要素は、アラームの概要がアラームと異なる点です。デバイスを選択すると、ページの下部の [Alarms and Events for *device*] ペインに、選択に対応するアラームとイベントが表示される。CSV または PDF ファイルとしてアラームをエクスポートできます。アラームをエクスポー

トするには、必要なアラームを選択し、[アラームの概要（Alarm Summary）] ペインの右上にあるエクスポート アイコンをクリックします。

[アラームの概要（Alarm Summary）] には、次の情報が表示されます。

重大度

アラーム重大度アイコン。アラームの重大度を示します。

直近 15 分

これがテーブル内の最新のデバイスの 1 つであることを示します（直近 15 分以内）。デバイスは最新のイベント ステータス変更時刻に基づいてソートされます。

デバイス名

デバイス名または IP アドレスです。

デバイス IP

デバイス IP です。クイック ビュー アイコンをクリックし、デバイス 360° ビューを起動します。

タイプ

デバイス タイプです。

重大度列

- [重大（Critical）]：重大なアラームの合計数。
- [やや重大（Major）]：やや重大なアラームの合計数。
- [軽度（Minor）]：軽度なアラームの合計数。
- [警告（Warning）]：警告アラームの総数。

最終更新時間

アラームがアップデートされた日付と時刻（アラームの繰り返し、アラーム確認応答、注釈の追加などのアクティビティを示します）。アラームは重大度でグループ化され、重大度別に、一番最後に変更されたアラームがリストの先頭になります。

エンドポイント名

識別しやすくするためにエンドポイントに割り当てられた名前です。デフォルトでは、[Endpoints Name] 列は非表示になっています。すべての列を表示するには、右上の隅にある [Settings] オプションをクリックします。

プライベート IP アドレス

Cisco Prime Collaboration Assurance が MSP モードでインストールされている場合は、デバイスのプライベート IP アドレスが表示されます。デフォルトでは、[Private IP Address] 列は非表示になっています。すべての列を表示するには、右上の隅にある [Settings] オプションをクリックします。

[Event]

イベント タブには次の情報が表示されます。

ID

イベントの固有の ID 番号。

重大度

イベントの重大度は、重大、やや重大、比較的重大ではない、警告、および情報のいずれかです。イベントリストを重大度別（昇順または降順）にソートするには、タイトルをクリックします。イベントがクリアされると、重大度は情報に変更されます。

ステータス

イベントの現在のステータスです。

イベント名

イベントの名前です。イベントの詳細を表示するには、クイック ビュー アイコンにマウスを合わせます。[Event Customization] ページに対して相互起動するには、[Customize Event] をクリックします。これにより、選択したイベントの詳細が表示されます。イベントの詳細を編集するには、イベントを展開して [Custom Rule] をクリックします。

顧客

Cisco Prime Collaboration Assurance を MSP モードでインストールした場合、そのデバイスを所有するカスタマーは [イベント（Events）] ペインに表示されます。

デバイス名

イベントの名前です。イベントの詳細を表示するには、イベント名にマウスを合わせます。

デバイス IP

デバイスの IP アドレスを表示します。リンクを使用して、エンドポイントまたはインフラストラクチャ デバイスを起動できます。

コンポーネント名

デバイス名、またはデバイス プール、インターフェイスなどのコンポーネントの名前。

最終更新日

イベントの発生日時を表示します。

デバイス タイプ

デバイスのタイプを表示します。

カテゴリ

会議、エンドポイントなどの、アラームが割り当てられたカテゴリを表示します。

説明

イベントの説明

エンドポイント名

識別しやすくするためにエンドポイントに割り当てられた名前です。デフォルトでは、[Endpoints Name] 列は非表示になっています。すべての列を表示するには、右上の隅にある [Settings] オプションをクリックします。

モデル

cat4506、ciscoMCS7828I などのデバイス モデルを表示します。

プライベート IP アドレス

Cisco Prime Collaboration Assurance を MSP モードでインストールした場合、デバイスのプライベート IP アドレスが表示されます。デフォルトでは、[Private IP Address] 列は非表示になっています。すべての列を表示するには、右上の隅にある [Settings] オプションをクリックします。

（注）
- 発生したイベントの最新の一覧を表示するには、更新アイコンをクリックします。
- Cisco Prime Collaboration Assurance を MSP モードでインストールした場合、デバイスが属しているカスタマーを参照することができます。
- 任意の時点で、[Alarm ブラウザ] または [Alarm 概要] を表示するには、右下のリンクをクリックします。

コール イベントの表示

Cisco Prime Collaboration Assurance には、Cisco TelePresence Management Suite（TMS）の情報イベントが表示されます。また、Cisco TelePresence System Profile MXP シリーズ デバイスである Cisco TelePresence Integrator C シリーズのコーデックと Cisco TelePresence Video Communication Server (VCS) のコール接続または接続解除された情報を表示します。

コール イベントは一度に 1 台のサポート対象デバイスのみについて表示できます。

コール イベントを表示するには:

ステップ 1 **Cisco Prime Collaboration リリース 11.5 以降の場合**

移行方法 **[インベントリ（Inventory）] > [インベントリ管理（Inventory Management）]**

ステップ 2 デバイスを選択し、**[Call Events]** をクリックします。

（注） コール イベントは、Cisco VCS、MXP、MCU デバイスおよびコーデックだけに表示されます。

ステップ 3 [Call Events] ページには次の詳細情報が表示されます。

MXP およびコーデックの場合：

- 開始時間：コールの開始時刻

- リモート サイト：コールが発信されたサイト
- コール状態
- 持続時間
- コールの方向：着信コールか発信コールか
- コール プロトコル：H323/SIP
- 暗号化モード
- 原因
- 帯域幅
- コール ID

VCS の場合：

- 時刻
- 送信元アドレス
- 送信元エイリアス
- 接続先
- 住所
- 接続先エイリアス
- 持続時間
- コール状態
- コール
- プロトコル
- 帯域幅
- コール タイプ

アラームとイベントに関する注意事項

1. ポーリング間隔に依存するアラームは、アラームが発生して次のポーリングの前に消去される場合があります。そのため、Cisco Prime Collaboration Assurance には報告されません。
2. **SIPTrunk Out Of Service（OOS）相関アラームの動作**：

SIP Trunk OOS：この相関アラームは、複数の SIPTrunk OOS アラームを追跡および結合し、クラスタ レベルで 1 つの関連付けられたアラームを生成するために導入されています。相関関係は、2 分間の時間ウィンドウで発生します。

相関アラームをクリアするための条件は、次のとおりです。

- SIPTrunk OOS 相関アラームは、InService Syslogs を処理して関連付けられている個々の SIPTrunk OOS アラームをクリアすることで、クリアされます。
- 時間ベースでクリアすることもでき、相関アラームは 24 時間後に自動的にクリアされます。

上記の条件を使用し、次のいずれかのシナリオで相関アラームをクリアすることができます。

シナリオ 1：

- SIPTrunk OOS アラームが、Cisco Prime Collaboration Assurance で発生します。
- 個々の SIPTrunk OOS アラームが関連付けられ、対応する SIPTrunk OOS 相関アラームがクラスタ レベルに上げられます。
- SIPTrunk OOS は SIPTrunks が戻るとクリアされ、対応する SIPTrunk OOS もクリアされます。

シナリオ 2：

- SIPTrunk OOS アラームが、Cisco Prime Collaboration Assurance で発生します。
- 個々の SIPTrunk OOS アラームが関連付けられ、対応する SIPTrunk OOS 相関アラームがクラスタ レベルに上げられます。
- SIPTrunk が 24 時間以上停止します。
- SIPTrunk OOS は、24 時間の時間ベースに基づき 24 時間後にクリアされ、SIPTrunk のサービスが再開して syslog が処理されると、SIPTrunk OOS の個々のアラームはクリアされます。

シナリオ 3：

- 個々の SIPTrunk OOS アラームが 2 分間の相関ウィンドウ内ですばやく生成され、クリアされます。
- 相関エンジンは依然として実行され、SIPTrunk OOS 相関アラームを発生しますが、対応する個別のアラームがすでにクリアされたため、SIPTrunk OOS はそのまま残ります。
- 次に、相関アラームは、24 時間の時間ベースに基づき 24 時間後に自動的にクリアされます。

3. マルチ ノード コール マネージャ クラスタでは、同じアラートが複数のノードに存在する場合、PCA は 1 つの新しいアラートを表示します。

4. RTMT アラートのポーリング頻度

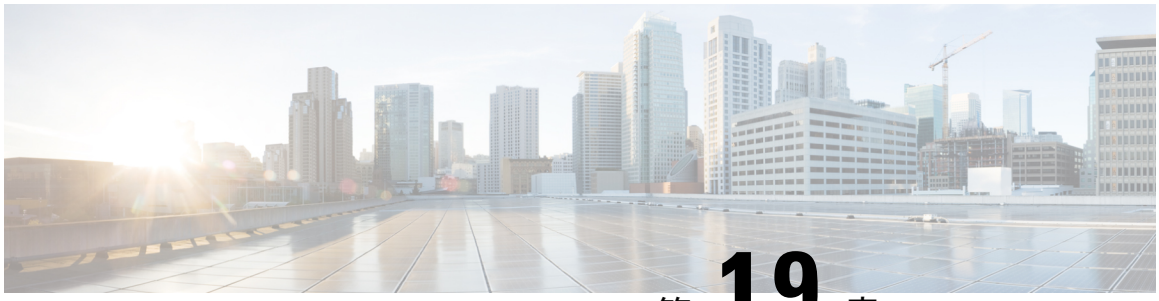
   Cisco Prime Collaboration リリース 12.1 以降の場合

   小、中、大のセットアップでは、RTMT アラートのデフォルトのポーリング頻度は 1 分となっており、特大の設定で推奨されるポーリング頻度は 2 分です。

第 V 部

ネットワークの監視

- ビデオ エンドポイントの監視 （301 ページ）
- 会議の監視 （311 ページ）
- Cisco APIC-EM を有効にして会議をトラブルシュート （341 ページ）
- Cisco Prime Collaboration Assurance サーバの監視 （345 ページ）



第 19 章

ビデオ エンドポイントの監視

このセクションでは、次の点について説明します。

- ビデオ エンドポイントの監視 （301 ページ）

ビデオ エンドポイントの監視

エンドポイントの診断ダッシュボードには、すべてののビデオエンドポイントの詳細が表示されます。

Cisco Prime Collaboration リリース 11.6 以降の場合

の任意のエンドポイントをウォッチリストに追加して、さらに詳細なトラブルシューティングを行うことができます。

[ウォッチリストに追加（Add to Watch List）] および [ウォッチリストから削除（Remove from Watch List）] は、エンドポイントの 360° ビューにも含まれています。[ウォッチリストに追加（Add to Watch List）] を使用すると、会議をウォッチリストに追加することができます。これは、[Not In Use] および [In Use] の両方のエンドポイントで有効です。ステータスが [Not In Use] のエンドポイントの場合、エンドポイントが会議に参加するとトラブルシューティングが開始されます。ステータスが [In Use] であるエンドポイントに対しては、ただちにトラブルシューティングが開始されます。

Cisco Prime Collaboration リリース 11.5 以降の場合

（注） より詳しいトラブルシューティングを行うために、すべてのエンドポイントをウォッチリストに追加する必要はありません。

ページの左側にある [Device Group] ペインを使用して、デバイス タイプに基づいてエンドポイントをフィルタリングすることができます。詳細については、「デバイス グループの管理」を参照してください。

エンドポイントの診断ダッシュボード

エンドポイントの診断ダッシュボードには、すべてのビデオエンドポイントの詳細が表示されます。

ページの左側にある [Device Group] ペインを使用して、デバイス タイプに基づいてエンドポイントをフィルタリングすることができます。詳細については、「デバイス グループの管理」を参照してください。

選択 **[診断（Diagnose）]** > **[エンドポイントの診断（Endpoint Diagnostics）]** をクリックして、エンドポイント診断ダッシュボードを表示します。次の表には、エンドポイントの診断ダッシュボードに表示される情報が示されています。

表 *48* : エンドポイントの診断ダッシュボード

情報	説明
エンドポイント サマリー メトリック	次の詳細を提供します。 • **Cisco Prime Collaboration リリース 11.1 以前の場合** 管理対象エンドポイント • 未登録のエンドポイント • 現在使用中のエンド ポイント • アラームのあるエンドポイント • 監視リストに追加されたエンドポイント
エンドポイントのリスト	すべての登録済み、未登録、不明なエンドポイントに関する詳細情報を提供します。エンドポイントの登録、使用状況、および可視性のステータスを確認するには、このペインを使用できます。
エンドポイントの詳細	選択したエンドポイント タイプに基づいて次の詳細を提供します。 • システム情報 • 周辺機器 • 次の 3 日間にスケジュールされた会議 • サービスおよびネットワーク インフラストラクチャ

（注） **Cisco Prime Collaboration リリース 11.5 以降の場合**

TC/CE ソフトウェアで実行される、ビデオまたは TelePresence ポイントに接続された周辺機器（カメラやマイクなど）の詳細を表示できます。これは、SX、MX、EX シリーズのエンドポイントに適用されます。

Cisco Prime Collaboration リリース 11.6 以降の場合

TC/CE ソフトウェアで実行される、ビデオまたは TelePresence ポイントに接続された周辺機器（カメラやマイクなど）の詳細を表示できます。これは、CE イメージを使用する SX、MX、DX、および EX 一連のエンドポイントに適用可能です。

CE イメージを使用する ciscoDX70 および ciscoDX80 はエンドポイント診断をサポートされていません。

Cisco Prime Collaboration Assurance を MSP モードで導入した場合、エンドポイントが属するお客様を確認できます。Cisco Prime Collaboration Assurance を Enterprise で導入した場合、エンドポイントが属する Assurance ドメインを確認できます。[モデル（Model）]、[デバイス プール（Device Pool）]、[クラスタ名（Cluster Name）]、[IP アドレスの切り替え（Switch IP Address）] 列をフィルタリングすることができます。[フィルタ（Filter）] アイコンをクリックし、これらの列でドロップダウン リストの矢印をクリックします。ポップアップ ウィンドウに一覧が表示されます。

エンドポイントの診断ダッシュボードは CSV または PDF ファイルとしてエクスポートできます。このファイルには、ユーザ インターフェイスに表示される正確なデータが含まれています。

クイック ビュー アイコンをクリックすると、エンドポイント 360° ビューが表示されます。

エンドポイントの可視性を変更するには、**[可視性の変更（Edit Visibility）]** をクリックします。

[エンドポイントの診断（Endpoint Diagnostics）] フィルタに保存されているフィルタは、正常に保存されません。保存されたフィルタは現在のセッションのみに存在し、更新/ログアウト後にクリアされます。

Cisco Prime Collaboration リリース 12.1 SP2 以降の場合

（注） 新規インストール（Cisco Prime Collaboration Assurance 12.1 SP2）では、エンドポイントの可視性設定はデフォルトで [OFF] 状態になっています。以前のバージョン（Cisco Prime Collaboration Assurance 11.6、Cisco Prime Collaboration Assurance 12.1 FCS/ES1/ES2/ES3/ES4/SP1/ など）から Cisco Prime Collaboration Assurance SP2 にアップグレードしているときに、インストールのルーチンでは、すでに管理されているエンドポイントのデフォルトの可視設定を保持します。

Cisco Prime Collaboration リリース 12.1 SP2 以降の場合

TC/CE エンドポイントの可視性を変更すると、選択したエンドポイントでフィードバック サブスクリプションにエラーがある場合、「1 つ以上の TC_CE エンドポイントにフィードバック サブスクリプションエラーがあります。[管理ステータスの原因列を確認してください（Check Management Status Reason）] という警告メッセージが表示されます。

エンドポイントの現在の可視性が表示されます。何らかの変更を加えた場合は、**[保存（Save）]** をクリックします。詳細については、エンドポイントのリアルタイム可視性を参照してください。エンドポイント名の直前にあるアイコンにポインタを合わせると、エンドポイントの可視性ステータスがエンドポイント 360° ビューで表示されます。

エンドポイント 360° ビューでは、**[ウォッチリストに追加（Add to Watch List）]** および **[ウォッチリストから削除（Remove from Watch List）]** も表示されます。**[ウォッチリストに追加（Add to Watch List）]** を使用すると、会議をウォッチリストに追加することができます。これは、[Not In Use] および [In Use] の両方のエンドポイントで有効です。[Not In Use] のエンドポイントの場合、エンドポイントがセッション会議に参加するとトラブルシューティングが開始します。ステータスが [In Use] であるエンドポイントに対しては、ただちにトラブルシューティングが開始されます。

エンドポイントでは、次のテストを実行できます。

- On-Demand Phone Test：エンドポイントを選択し、**「テストの実行および音声電話機の機能テスト（Run Tests > Audio Phone Feature Test）]** をクリックします。On-Demand Phone Test の詳細については、Phone Test：Batch および On Demand Test を参照してください。
- Synthetic - End-to-End Call Test：エンドポイントを選択し、**[テストの実行および音声テスト コール（Run Tests > Audio Test Call）]** をクリックします。End-to-End Call Test テストの詳細については、End-to-End Call Synthetic Test の作成 を参照してください。
- Video Test Call：2 つのビデオ エンドポイントを選択し、**[テストの実行および音声テスト コール（Run Tests > Video Test Call）]** をクリックします。Video Test Call の詳細については、ビデオ テスト コールの管理を参照してください。

（注） Cisco Prime Collaboration Assurance を MSP モードで導入した場合、[Video Test Call] 機能は使用できません。

不明なエンドポイントの一覧を表示するには、ユーザ インターフェイスの左側にある [デバイス グループ セレクタ（Device Group Selector）] ペインで [定義済みおよび不明なエンドポイント（Predefined > Unknown Endpoints）] を選択します。

（注） Polycom エンドポイントは Cisco VCS に登録されている場合だけをモニタされます。Polycom コール コントローラに登録されたときにはモニタされません。自動コール検出は HTTP フィードバックを使用してサポートされます（Cisco VCS を使用します）。会議の統計や会議の情報など、リアルタイムのモニタリングに関する情報はサポートされていません。

デフォルトでは、[エンドポイントの診断（Endpoints Diagnostics）] ページの自動更新機能は無効になっています。2 分ごとの自動更新を有効または無効にするには、ユーザ インターフェイスの右上隅にある **[自動更新（Auto Refresh）]** チェックボックスをオンにします。

自動更新機能を無効にし、後でアプリケーションにログインすると、機能は無効のままになっています。有効にするには、**[自動更新（Auto Refresh）]** チェックボックスを再度オンにします。

（注） **Cisco Prime Collaboration リリース 11.5 以降の場合**

音声またはビデオのエンドポイントが 1 つの Unified Communications Manager クラスタから別の Unified Communications Manager クラスタに移動すると、Cisco Prime Collaboration Assurance は、エンドポイントが現在登録されているクラスタのデバイス情報のみを表示します。いくつかのフィールド（例：デバイス プール）のデバイス情報は、夜間に実行されるクラスタ検出の後に表示されます。そのため Cisco Prime Collaboration Assurance は、以前の Unified Communications Manager クラスタと現在のクラスタの間で数が一致しない未登録のエンドポイントを表示します。以前のエントリが Unified Communications Manager にパージされると、正しい数の未登録のエンドポイントが表示されます。

ユーザ詳細の 360° ビューを表示

このビューには、Cisco Unified Communications Manager または Cisco TelePresence Management Suite（TMS）エンドポイントに関連付けられているエンドユーザの情報（ユーザ名、電子メール ID、オフィス電話番号、携帯電話番号など）が表示されます。エンドユーザの写真とロケーションの詳細は、Cisco Prime Collaboration Assurance が LDAP と統合されていて、ユーザ名詳細が LDAP 詳細と一致している場合にのみ表示されます。

（注） TMS に関連付けられているエンドユーザ情報は、「TMS プロビジョニング拡張機能」コンポーネントが TMS にインストールされている場合にのみ取得できます。

このビューにアクセスするには、以下を行います。

ステップ 1 グローバル検索ドロップダウンから、[ユーザ（User）] を選択します。[**エンドポイントの診断（Endpoint Diagnostics**）] ページの [ユーザ名（Username）] 列から ユーザ 360 を起動することもできます。

ステップ 2 ***** を入力すると、すべてのユーザが一覧表示されます。文字列検索によって、より具体的な結果を得ることができます。たとえば、**test** と入力すると、名、姓、またはユーザ名に「test」という文字列が含まれているすべてのユーザが一覧表示されます。

ステップ 3 ユーザ名に対応する [ユーザ 360 ビュー（User 360 View）] 起動アンカーをクリックします。

このビューの以下のタブにアクセスします。

- [エンドポイント（Endpoints）]：エンドユーザに関連付けられている管理対象エンドポイントが表示されます。このエンドポイントには、次が含まれます。
  - [前回の通話品質（Last Call Quality）]：good、accepted、poor に分類されます。このフィールドには、最後に終了したコールの通話品質が示されています。CUCM に登録されているエンドポイントの **[CMR レポート（CMR Report）]**、または TMS に登録されているエンドポイントの [アラーム（Alarms）] ページを起動できます。
  - コール（24 時間）：過去 24 時間に発生した、エンドポイントが関与したコールの数。このフィールドは、Unified CM に登録されたエンドポイントの **CDR レポート**、および TMS に登録されたエンドポイントの**全会議サマリー レポート**から、を起動できます。
  - [登録ステータス（Registration Status）]：エンドユーザの登録ステータスが表示されます。コールが進行中の登録済みエンドユーザの場合、コール進行中インジケータである緑色のアイコンが表示されます。登録されていないエンドユーザの場合は赤色のアイコンが表示され、エンドユーザのステータスが不明な場合はグレーのアイコンが表示されます。
  - [サービス（Service）]：最後に終了したコールのサービス（音声のみ、または音声とビデオ）。
  - [エンドポイントモデル（Endpoint Model）]：エンドポイント モデルが表示されます。クリックすると、[**エンドポイントの診断（Endpoint Diagnostics**）] ページを起動します。
- [アクティブ会議（Active Conferences）]：現在通話中のエンドユーザのエンドポイントが表示されます。デバイスの詳細は、会議診断から追跡されます。[アクティブ会議（Active Conferences）]には次のものが含まれています。
  - エンドポイントと接続先番号の画像。画像をクリックすると、[**エンドポイントの診断（Endpoint Diagnostics**）] ページが起動されます。
  - [品質統計（Quality stats）]：通話品質アラームの現在の最高重大度を示すアラーム アイコン。
  - **Cisco Prime Collaboration リリース 11.1 以前の場合**

    [ツール（Tools）]：トラブルシューティング ページへのリンク。
- [アラーム（Alarms）]：以下を表示します。
  - Severity
  - アラームを受信したソース
  - アラームの名前
  - タイムスタンプ

（注） Unified CM に登録されているエンドポイントの場合は、新しいユーザの同期が自動的に行われます。TMS に登録されたエンドポイントを除いて、新しいユーザの詳細を同期するには、TMS を手動で再検出する必要があります。

ビデオ テスト コールの管理

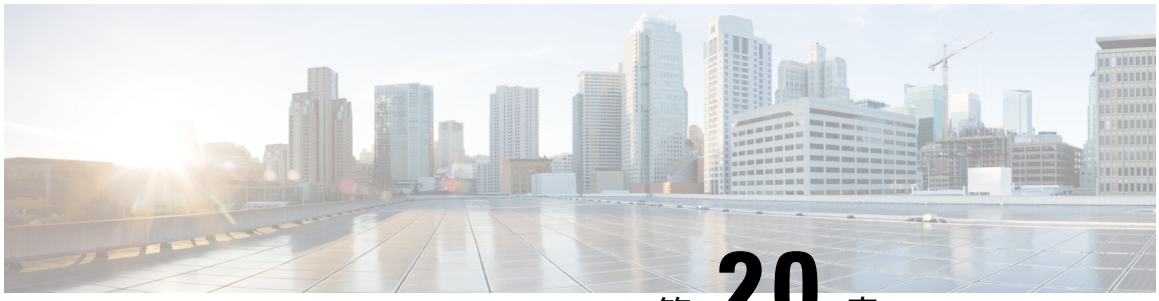
Managed の状態にある 2 つのビデオエンドポイント間で、ビデオテスト コールをポイントツーポイントで作成し、ネットワークをテストすることができます。Medianet の統計を使用し、イベントとアラーム、会議の統計、エンドポイントの統計。このコールでは、CTS、C および EX シリーズのコーデックのみがサポートされています。

（注）
- この機能は、E20 のコーデック シリーズではサポートされていません。
- この機能を使用するには、エンドポイントの CLI クレデンシャルを追加する必要があります。
- エンドポイントが登録済みであり、（Unified CM に登録されている）エンドポイントで JTAPI が有効になっていることを確認してください。
- Cisco Prime Collaboration Assurance を MSP モードで展開している場合は、ビデオ テスト コール機能は使用できません。
- Mobile and Remote Access（MRA）ソリューションを使用してエンドポイントが登録されている場合、「ビデオ テスト コール」機能はサポートされません。

表 *49 :* ビデオ テスト コールの管理

タスク	説明
• [**診断**（**Diagnose**）] の [**エンドポイントの診断**（**Endpoint Diagnostics**）]で、ビデオ テスト コールを開始する • ビデオ テスト コールを開始する [**診断**（**Diagnose**）] の [**会議の診断**（**Conference Diagnostics**）]	ビデオのエンドポイントを選択し、[ビデオテストコール（Video Test Call）] をクリックして、選択した 2 つのエンドポイント間にテスト コールを作成します。 （注） • このボタンは、ビデオのエンドポイントを 2 つ選択した後にのみ有効になります。 • エンドポイントを 2 つよりも多く選択して、ビデオ テスト コールを作成することはできません。 または [会議の診断（Conference Diagnostic）] ページで会議を選択し、[ビデオテストコール（Video Test Call）] をクリックして、そのスケジュール済みの会議に対してテスト コールを作成します。 （注） このボタンは、スケジュール済みの会議を選択した後にのみアクティブになります。スケジュール済みの会議のリストを表示するには、スケジュール済みの会議で絞り込みます。日時が現時点よりも先の会議のみを選択してください。 [テストコールの追加（Add Test Call）] ウィンドウが表示され、エンドポイントの IP アドレスをクリックすると、そのアプリケーションが起動します。デフォルトでは、テスト コールは即座に実行されますが、スケジュールを設定することもできます。 CTS エンドポイントの場合は、SIP プロトコルのみを選択してください。Ex および C シリーズのエンドポイントの場合、H.323 と SIP のいずれかのプロトコルを選択できますが、これらのエンドポイントがこれらのプロトコルを使用して登録されている必要があります。[コールの追加（Add Call）] ボタンをクリックすると、コールが正常に追加されたことを通知するメッセージが表示されます。 スケジュール済みのコールの詳細を、[会議の診断（Conference Diagnostics）] ページで確認できます。Medianet の統計を使用し、イベントとアラーム、会議の統計、エンドポイントの統計。この情報は、テスト コールが完了した後でも確認できます。コールによってネットワークの問題が発生した場合は、すぐにコールを停止することができます。

タスク	説明
実行中のビデオテストコールの停止	ビデオ テスト コールによってネットワークに問題が起きた場合は、コールを停止することができます。コールを停止するには、[会議の診断（Conferences Diagnostic）] ページでフィルタに [テストコール会議（Test Call Conferences）] を設定して、テストするコールを選択します。会議の件名にマウス カーソルを合わせると、360° 会議ビューが表示され、[コール停止（Stop Call）] アイコンをクリックすると、進行中のビデオ テスト コールが停止します。 テスト コールは約 5 分間継続し、その後自動的に停止します。
スケジュール済みのビデオ テスト コールを [ビデオ テスト コールの設定（Video Test Call Configurations）] ページで編集する **[模擬テスト（Synthetic Tests）] > [ビデオ テスト（Video Test）]** 同じページからビデオテストコールを表示または削除することもできます。	[編集（Edit）] をクリックしてビデオ テスト コールを編集し、[保存（Save）] をクリックするとコールを再スケジュールまたは即座に実行できます。コールが正常に変更されたことを通知するメッセージが表示されます。



第 20 章

会議の監視

このセクションでは、次の点について説明します。

- 会議の監視 （311 ページ）

会議の監視

Cisco Prime Collaboration リリース 11.5 以降の場合

Cisco Prime Collaboration Assurance は、ネットワーク内のビデオ コラボレーション会議のライフサイクルを追跡します。これはさまざまなソースから受信した会議データを関連づけ、会議に関するエンド ツー エンドの詳細情報を提供します。

Cisco Prime Collaboration Assurance は、Cisco Unified CM や Cisco TelePresence Video Communication Server（VCS）など、コールおよび会議制御コンポーネントから会議イベントを受信します。また、管理アプリケーション、コールおよび会議制御コンポーネント、会議コンポーネント、エンドポイントなどのアプリケーションから会議の詳細を取得します。

Cisco Prime Collaboration Assurance が監視可能な会議数は、小規模や中規模などの導入モデルによって異なります。サポートされているアクティブな会議の詳細については、「System Capacity for Cisco Prime Collaboration Assurance 用のシステム容量」を参照してください。

（注） 150k および 80k プロファイルでは、JTAPI を使用してすべてのエンドポイントを制御し、Cisco Prime Collaboration Assurance でデバイスを検出すると、[OutofMemory] 状態となりサーバがクラッシュします。したがって、セッション機能を監視するために必要なエンドポイントのみを追加します。

ビデオ コラボレーション アプリケーションから取得される会議データには、スケジュールされたおよびスケジュールされていない会議の両方が含まれます。Cisco Prime Collaboration Assurance は、次の方法で会議を区別します。

- Ad hoc - エンドユーザは、相手側で Cisco TelePresence システムの内線番号をダイヤルします。スケジューリングは関係しません。

- スケジュール済み - Microsoft Exchange や Outlook など、企業のグループウェア アプリケーションを介して会議前にスケジュールします。また、Cisco TelePresence Management Suite（TMS）を使用して会議をスケジュール設定することもできます。
- スタティック - 事前設定済みの Cisco TelePresence 会議を常時使用できます。各スタティック会議は独自の会議番号が関連付けられています。Cisco TelePresence MSE、Multipoint Control Unit（MCU）、Cisco TelePresence Server（TS）などの一部のアプリケーションでは、このようなミーティングを永続的な会議と呼びます。

Cisco Prime Collaboration Assurance では、次のように会議構造を分類します。

- Point-to-point - 2 つのエンドポイント間の会議です。
- Multipoint - 2 つ以上のエンドポイントを持つ会議です。エンドポイント間には、MCU が存在する場合があります。
- MultiSite - MCU がない 2 つ以上のエンドポイントがある会議です。エンドポイントは直接接続されます。すべてのエンドポイントは、MultiSite 対応のセンターエンドポイントを使用して MultiSite コールに参加できます。センター エンドポイントは会議デバイス（MCU など）のように機能します。このタイプの会議構造は、Cisco Codec C、TelePresence System EX シリーズ、Cisco TelePresence MX シリーズ、MultiSite ライセンスの Cisco プロファイル シリーズなど、MultiSite 対応のエンドポイントでサポートされています。

会議のステータスは、次のとおりです。

- In-progress
- Scheduled
- Completed
- [No Show] とは、終了時間まで参加者が会議に参加することのなかったスケジュール済み会議です。スケジュール済み会議は、スケジュールされた終了時間の後、ならびにスケジュールされた終了時間の後で Cisco Prime Collaboration Assurance が Cisco TMS と同期した後のみに、[No Show] へと変わります。

エンドポイントが進行中の会議に参加しなかった場合、エンドポイントには [不参加（No Show）] アイコンが表示されます。このステータスは、会議が [Completed] 状態に移行した後でも表示されます。

1 つのエンドポイントが会議に参加していても、会議が終了する前にコールから切断した場合、会議トポロジのこのエンドポイントには切断アイコンが表示されます。切断とは、何らかの問題があったか、発信者が会議を早く終了する必要があったことを意味する場合があります。

Cisco Prime Collaboration リリース 12.1 SP2 以降の場合

会議の診断の前提条件

会議の診断には、次の前提条件があります。

- Unified CM および Cisco VCS は、Managed 状態にある必要があります。

- MCU などのエンドポイントとコントローラは、Managed 状態にある必要があります。
- デバイスの可視性を 「Full Visibility」 状態に設定します。
- JTAPI が Unified Communications Manager で設定されている必要があります。Unified Communications Manager で JTAPI を有効にする方法については、「Cisco Prime Collaboration Assurance のデバイス設定」を参照してください。
- Cisco Prime Collaboration Assurance サーバが、Cisco VCS でフィードバック サーバとして登録されている必要があります。
- Cisco Prime Collaboration Assurance で TC/CE デバイス タイプとして検出された Cisco Telepresence エンドポイントは、JTAPI ユーザーが制御するデバイス リストには含めないようにします。IP フォンは、JTAPI ユーザの制御リストで保持することを推奨します。
- 会議の診断機能は、エンドポイントから直接送信された HTTPS フィードバックを使用し、CUCM が登録された Telepresence（TC/CE）エンドポイントのみをサポートしています。
- 会議の診断は、エンドポイントでサブスクリプションが失敗した場合には機能しません。
- 会議の診断と音声電話機能の合成テストを使用するには、Cisco Prime Collaboration Assurance Service Pack 1 を適用する前に、CUCM が一覧表示されたバージョンであることを確認します。詳細については、12.1 Service Pack 1 の「Cisco Prime Collaboration Assurance でサポートされているデバイス」を参照してください。

（注）

1. Cisco Prime Collaboration Assurance は、Unified Communications Manager に登録済みの Cisco Jabber エンドポイントに対する会議監視はサポートしていません。使用率レポートおよび TelePresence（Movi）エンドポイント用 Cisco Jabber Video の使用統計のみが表示されます。
2. セッション インポート ポーリングのデフォルト間隔は 24 時間です。
3. JTAPI には TS および TX エンドポイントが含まれていないことを確認します。

ビデオ会議のデータ収集

Cisco Prime Collaboration Assurance は、次のビデオ サービス インフラストラクチャ デバイスを定期的にポーリングして、会議に関する情報を取得します。

- 管理デバイス（Cisco TMS）：Cisco Prime Collaboration Assurance は、スケジュール済みポイント ツー ポイント会議とマルチポイント会議に関する情報を取得します。Cisco TMS では、会議の進行中にスケジュール設定されていないエンドポイントが追加されると、Cisco Prime Collaboration Assurance は新しく追加されたエンドポイントの会議の詳細を表示します。

  Cisco Prime Collaboration Assurance は 5 日分のスケジュール済み会議のデータを収集します（前日、当日および今後 3 日）。

（注） Cisco TMS 13.0 または 13.1 を使用している場合は、予約 API 機能を設定します。Cisco TMS 13.2 以上の場合は、Booking API 機能を設定する必要はありません。

- マルチポイント スイッチ：Cisco Prime Collaboration Assurance は、マルチポイント会議の情報を取得します。また、マルチポイント会議のカスケードの特定とサポートも行います。
- マルチポイント コントロール ユニット（MCU および Cisco TS）：これらのシステムを使用してスケジュールされた会議は、Cisco Prime Collaboration Assurance では常にアドホック会議としてリストされます。これらのタイプの会議は、会議の開始後にのみ [会議の監視（Conference Monitoring）] ページに一覧表されます。Cisco Prime Collaboration Assurance は、エンドポイントからイベントを受信した後、これらのシステムにポーリングします。

  Cisco Prime Collaboration Assurance では、これらのシステムがコールを受信するたびに、MCU と Cisco TS をポーリングします。Cisco Prime Collaboration Assurance は、Cisco TelePresence Conductor によって管理されていない MCU をポーリングします。

  Cisco TelePresence Conductor で制御される MCU によってホストされている会議の場合、Cisco Prime Collaboration Assurance が Cisco TelePresence Conductor のみをポーリングします。

  Cisco Prime Collaboration Assurance は MCU 会議のカスケードをサポートしません。Cisco TelePresence Conductor が制御する MCU のカスケードのみがサポートされます。
- コールおよび会議制御（Cisco Unified CM および Cisco VCS）：Cisco Prime Collaboration Assurance は、コール プロセッサを使用して参加者に関する情報を取得します。ユーザの会議への加入時間や切断時間といった詳細事項が収集されます。Cisco Prime Collaboration Assurance はコールと会議コントローラを定期的にポーリングします。

  Cisco Prime Collaboration Assurance は、Cisco Unified CM および Cisco VCS からリアルタイムで接続/切断イベントを受け取ります。接続/切断イベントが失われた場合、バックアップ メカニズムとして、Cisco Prime Collaboration Assurance はすべての進行中のコールに対して定期的に Cisco Unified CM と Cisco VCS をポーリングします。その結果、これらは同期されます。

Cisco Prime Collaboration リリース 12.1 SP2 以降の場合

Cisco Prime Collaboration Assuranceは、[Connect（接続）] または [Disconnect（切断）] イベントを、Cisoc Unified Communications Manager JTAPI ではなくエンドポイント（(TC/CE）からリアルタイムに受信します。

（注） 会議のモニタリング ウィンドウでは、次のブラウザがサポートされています。

- Internet Explorer：バージョン 10、11
- Mozilla Firefox：バージョン 31、38
- Google Chrome：バージョン 39、40

Cisco Unified CM

すべてのエンドポイントが、Cisco Unified CM に JTAPI 制御対象デバイスとして追加されている必要があります。追加されていない場合、Cisco Prime Collaboration Assurance でエンドポイントの通話検出は発生しません。設定された JTAPI ユーザは、Cisco Prime Collaboration Assurance で管理されるすべてのエンドポイントへのアクセスを許可されている必要があります。

Cisco Prime Collaboration Assurance は、Cisco Unified CM からの JTAPI イベントをリッスンします。コールが進行中になると、エンドポイントがポーリングされます。Cisco Prime Collaboration Assurance は、JTAPI イベントに依存して会議を完了ステータスへ移行します。

Cisco Prime Collaboration Assurance は、複数の Cisco Unified CM クラスタを管理します。クラスタ内およびクラスタ間の会議（クラスタ内およびクラスタ間会議）を監視するために一意のクラスタ ID を設定します。

Cisco Prime Collaboration Assurance は、クラスタをモニタリングするためにクラスタ パブリッシャを管理する必要があります。JTAPI はクラスタ パブリッシャで設定する必要があり、コンピュータ テレフォニー インテグレーション（CTI）サービスがクラスタ内の少なくとも 1 つのノードで動作している必要があります。CTI 制御 は、デバイスに設定された完全な可視性によって異なります。可視性の制限については、「Cisco Prime Collaboration Assurance のシステム容量」を参照してください。

JTAPI が Cisco Unified CM に設定されていない場合、その JTAPI に登録されたエンドポイントは会議の一部として表示されません。この場合は、JTAPI 設定を設定します。

（注） JTAPI 制御対象デバイスとして追加されたエンドポイントの正しい使用状況の詳細を表示し、エンドポイントを Cisco Unified CM のコントロール リストに表示するには、エンドポイントの可視性をリセットする必要があります。**[診断（Diagnose）]>[エンドポイントの診断（Endpoint Diagnostics）]** の下の [可視性の編集（Edit Visibility）] を使用して、エンドポイントの可視性を [完全な可視性（Full Visibilty）] から[オフ（Off）]に変更し、その後、再度 [完全な可視性（Full Visibilty）] に切り替えます。

また、Cisco Unified CM を再検出してエンドポイントを見えるようにし、Cisco Prime Collaboration Assurance サーバでの正しい使用ステータスを表示することもできます。

Cisco Prime Collaboration リリース 12.1 SP2 以降の場合

Cisco TC/CE

Cisco Unifired Communications Manager に登録されている Cisco TC/CE エンドポイントの場合、イベントは Unified Communications Manager JTAPI ではなくエンドポイントから直接受信します。

Cisco VCS

Cisco Prime Collaboration Assurance は、Cisco VCS からの HTTP フィードバック イベントをリッスンします。コールが進行中になると、エンドポイントがポーリングされます。Cisco Prime Collaboration Assurance は、HTTP フィードバック イベントに依存して、会議を完了ステータスに移行します。

Cisco Prime Collaboration Assurance は、複数の Cisco VCS クラスタを管理します。クラスタ内およびクラスタ間の会議（クラスタ内およびクラスタ間会議）を監視するために、一意のクラスタ名を設定する必要があります。

Cisco Prime Collaboration Assurance は、Cisco VCS Expressway トラバーサル コールを識別し、サポートします。これらのコールについて、Cisco VCS Control と Cisco VCS を使用してメディアが信号通知を行い、コールの詳細は、会議トポロジで表示されます。

トラバーサル コールの詳細については、Cisco TelePresence Video Communication Server Control のオンライン ヘルプを参照してください。

エンタープライズ ファイアウォールの外へのコールがある場合は、Cisco VCS Expressway を使用します。このデバイスは、Cisco VCS Control デバイスに設定します。Cisco VCS Control および Cisco VCS Expressway は、会議トポロジに表示されます。ただし、Cisco VCS Expressway に登録されたエンドポイントは、不明なエンドポイントとして表示されます。

Cisco Prime Collaboration Assurance がフィードバック サブスクリプションによって VCS に登録されていない場合、登録エンドポイントが会議に参加または退室したとき、または VCS に登録または登録解除されたときに、VCS は PCA に通知しません。この場合、必要に応じて、エンドポイントの可視性を [完全（full）] に設定し、ネットワーク管理者に連絡して、VCS への PC のフィードバック サブスクリプションを確認します。

（注） Cisco Prime Collaboration Assurance では、Cisco VCS Expressway の接続/切断イベントが無視されます。

Cisco TMS から会議のインポート

Cisco TMS には、スケジュールされた会議の詳細が含まれています。Cisco Prime Collaboration Assurance は、定期的にこれらのデバイスをポーリングして、会議の詳細を取得します。定期的なポーリングの頻度は、ビジネスのニーズに合わせて設定できます。

会議を中断なく使用するには、[クラスタの管理（Manage Clusters）] オプション（**[インベントリ（Inventory）]** > **[インベントリ管理（Inventory Management）]** > **[TMS クラスタの管理（Manage TMS Clusters）]**。

Cisco TMS では、スケジュール済み会議の進行中にスケジュール設定されていないエンドポイントが追加されると、Cisco Prime Collaboration Assurance では、追加されたエンドポイントの会議の詳細が表示されます。

Cisco Prime Collaboration Assurance は 5 日分のスケジュール済み会議のデータをインポートします（前日、当日および翌 3 日間）。

Cisco TMS から会議をインポートするときは、次の点に注意してください。

- Cisco Prime Collaboration Assurance は、Cisco TMS の予約確認メールで、デフォルトの電子メール テンプレートのみをサポートしています。デフォルトの電子メール テンプレートを使用していない場合、会議は Cisco TMS からインポートされません。
- 「予約のみ」の会議の詳細は、Cisco TMS からインポートされません。Cisco Prime Collaboration Assurance は、スケジュールの設定中にリソースが割り当てられないため、このタイプのミーティングはサポートしていません。

定期的なポーリング以外にも、会議の詳細をすぐにインポートする場合は、**[診断（Diagnose）]**> **[会議の診断（Conference Diagnostics）]** > **[会議のインポート（Import Conferences）]**。

（注） [会議のインポート（Import Conferences）] タスクは、Cisco Prime Collaboration Assurance System システムのパフォーマンスに影響を及ぼします。必要な場合のみ、[会議のインポート（Import Conferences）] を使用します。

[会議のインポート（Import Conferences）] タスクでは 1 つのジョブが作成されます。これは、**[システム管理（System Administration）]、** > **[ジョブ管理（Job Management）]** から監視できます。ジョブ タイプは、[ジョブ管理（）] ページでは Synch_TMS-MEETING_UniqueJobID として表示されます。

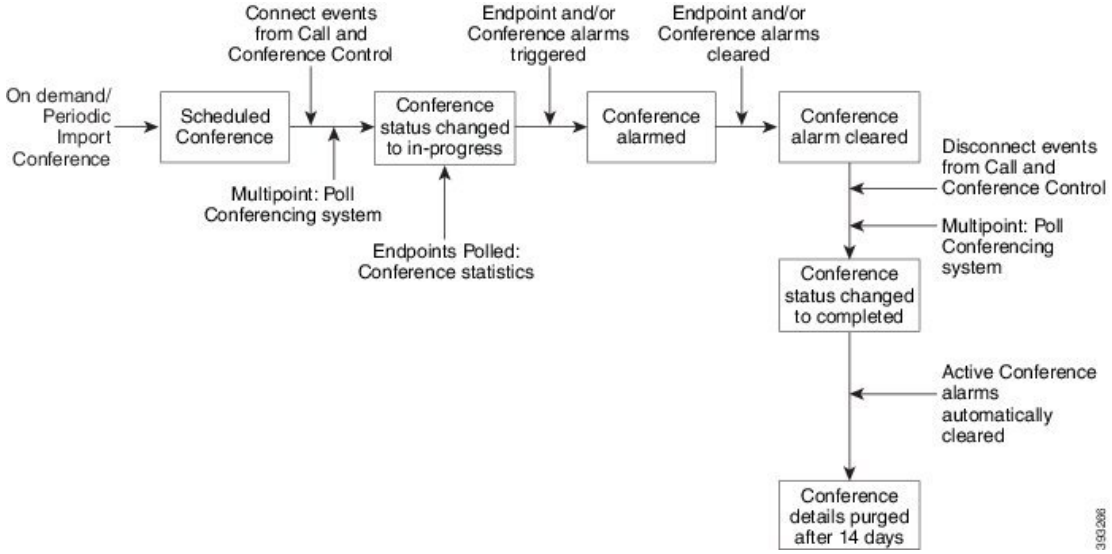
TMS_Conference_Import はジョブを定期的に実行し、すべての会議の詳細をポーリングします。

ただし、TMS_Frequent_Conference_Import ジョブは頻繁に実行され、前回のポーリング後の会議の変更のみを取得します。（ポーリングの頻度は、[システム セットアップ（System Setup）] ページで変更できます）。

会議のワークフローとシナリオ

次の図には、エンド ツー エンドによるスケジュール済み会議のワークフローが示されています。

図 *4:* スケジュール済み会議のワークフロー



次のシナリオでは、Cisco Prime Collaboration Assurance に会議の最新情報が含まれていない、または異なる会議の構造データが表示されています。

- Cisco Prime Collaboration Assurance では、会議が前回の Cisco TMS のポーリング後、ならびに次回のスケジュール設定またはオンデマンドによる Cisco TMS のポーリングが発生する前にスケジュール設定され、進行中とされた場合、スケジュール済み会議（ポイント ツー ポイント、マルチポイント、またはマルチサイト）をアドホック 会議として表示します。
- スケジュール設定済みマルチポイント会議では、Cisco Prime Collaboration Assurance が管理アプリケーションと同期されていない場合、会議はアドホックセッションとして表示され、Cisco Prime Collaboration Assurance は [接続（Connect）] イベントを受信した後に、参加している Cisco MCU から情報を収集します。
- 会議システムが Managed 状態から Unmanaged または Unknown 状態に移行した場合、マルチポイント会議は複数のポイント ツー ポイント会議として表示されます。
- Cisco TMS と Cisco MCU では、スケジュールされた時間が経過すると、会議ステータスがすぐに [アクティブ（Active）] に切り替わります。ただし、Cisco Prime Collaboration Assurance では、エンドポイントが会議に参加するまで会議ステータスが [進行中（In Progress）] に変わることはありません。
- Cisco Prime Collaboration Assurance では、管理されていないエンドポイントを含む会議が表示されます。だだし、これらのオプションの内容に注意してください。
  - ポイント ツー ポイント会議では、Cisco Prime Collaboration Assurance でいずれかのエンドポイントを管理する必要があります。
  - マルチサイト会議では、Cisco Prime Collaboration Assurance で、他のエンドポイントにて会議するエンドポイントを管理する必要があります。

- マルチポイント会議では、Cisco Prime Collaboration Assurance で会議デバイスを管理する必要があります。

- Cisco TMS を使用して TelePresence ルームのみを予約した場合、Cisco Prime Collaboration Assurance でこれらの会議が表示されることはありません。（Cisco TMS では、このような電話会議のタイプは *[*予約のみ（*Reservation Only*）*]* として識別されます）。
- Cisco VCS Expressway が Inaccessible 状態である場合でも、Cisco Prime Collaboration Assurance は会議を監視できます。ただし、エンドポイントは「不明」なエンドポイントとして表示されます。
- 会議の診断機能は、Cisco Unified Communications Manager で複数の回線を使用して設定されたエンドポイントはサポートしません。ただし、これらのエンドポイントは、Cisco Prime Collaboration Assurance インベントリ データベースで管理することができます。

（注） 会議の監視機能は、Cisco Unified CM 8.5 以降のみでサポートされています。

- TelePresence と複数の Webex 参加者の間に会議がある場合、[会議の診断（Conference Diagnostics）] ページには、コールで利用可能な Webex 参加者の詳細は表示されません。
- Cisco VCS（ポリシーサービス）導入による Cisco TelePresence Conductor がサポートされています。Cisco VCS（B2BUA）搭載 および Cisco Unified CM 導入による の Cisco TelePresence Conductor はサポートされていません。

会議シナリオ

Cisco Prime Collaboration Assurance で監視されるさまざまな会議シナリオは、次のとおりです。

表 *50* : 会議シナリオ

会議の分類	会議タイプ	会議構造	会議トポロジの要素
Cisco Unified CM のクラスタ内およびクラスタ間会議	アドホック、 スケジュール済み	ポイント ツー ポイント	Cisco TelePresence System 500、1000、3000、TX9000 シリーズ。
Cisco Unified CM のクラスタ内およびクラスタ間会議	アドホック、 スケジュール済み 静的	マルチポイント	Cisco TelePresence System 500、1000、3000、TX9000 シリーズ。

会議の分類	会議タイプ	会議構造	会議トポロジの要素
Cisco VCS クラスタ内およびクラスタ間会議	アドホック、スケジュール済み	ポイント ツー ポイント	Cisco C シリーズ、EX シリーズ、Cisco MX シリーズ、Cisco MXP、Cisco IP Video Phone E20、および Cisco Jabber。 コールがトラバーサルコールとして識別される場合は、Cisco VCS Control や Cisco VCS Expressway が会議トポロジに表示されます。
Cisco VCS のクラスタ内およびクラスタ間会議（MCU あり）	アドホック、スケジュール済み永続（静的として表示）	マルチポイント	Cisco C シリーズ、EX シリーズ、Cisco MCU、Cisco MSE[1]、または Cisco TelePresence Server。 コールがトラバーサルコールとして識別される場合は、Cisco VCS Control や Cisco VCS Expressway が会議トポロジに表示されます。
Cisco VCS のクラスタ内およびクラスタ間会議（MCU なし）	アドホック、スケジュール済み	マルチサイト	Cisco C シリーズ、EX シリーズ、Cisco MX、Cisco MXP シリーズ、Cisco IP Video Phone E20。 コールがトラバーサルコールとして識別される場合は、Cisco VCS Control や Cisco VCS Expressway が会議トポロジに表示されます。

会議の分類	会議タイプ	会議構造	会議トポロジの要素
Cisco Unified CM および Cisco VCS クラスタ間の会議 [2]	アドホック	ポイント ツー ポイント マルチポイント	• Cisco C シリーズ、EX シリーズ、Cisco MX シリーズ、Cisco MXP シリーズ、Cisco IP Video Phone E20 • Cisco TelePresence System 500、1000、3000、および TX9000 シリーズ。 • Cisco TelePresence Server • IX 5000 シリーズ TelePresence エンドポイント
Cisco Unified CM (8.6(1)、8.6(2)、9.0) のクラスタ内会議	アドホック	ポイント ツー ポイント	• Cisco C シリーズ、EX シリーズ、Cisco MX シリーズ • Cisco TelePresence System 500、1000、3000、および TX9000 シリーズ。 • IX 5000 シリーズ TelePresence エンドポイント

会議の分類	会議タイプ	会議構造	会議トポロジの要素
Cisco Unified CM（8.6(1), 8.6(2), and 9.0）のクラスタ内会議	アドホック、スケジュール済み （注） スケジューラは、1.7、1.8、または 1.9 である必要があります。	マルチポイント	• Cisco C シリーズ、EX シリーズ、Cisco MX シリーズ、Cisco IP Video Phone E20 • Cisco TelePresence System 500、1000、3000、および TX9000 シリーズ。 • 1.8 または Cisco TelePresence サーバ
エンタープライズファイアウォール外の会議：Cisco VCS Expressway	アドホック、永続（静的として表示）	ポイントツーポイント、マルチポイント、マルチサイト	• Cisco C シリーズ、EX シリーズ、Cisco MX シリーズ、Cisco MXP シリーズ、Cisco IP Video Phone E20 • Cisco MCU または Cisco TelePresence Server • Cisco VCS Control および Cisco VCS Expressway

会議の分類	会議タイプ	会議構造	会議トポロジの要素
コールのエンドポイント（コールに MCU あり）は、Cisco Unified CM で会議ブリッジとして機能します。	アドホック	ポイント ツー ポイント コールを会議モードにする、または別のコールとマージさせると、コールがマルチポイントになります。会議には、MCU が表示されません。最初の参加者がコールから離れると、会議は MCU に接続済みと表示されますが、2 番目と 3 番目の参加者は ポイント ツー ポイント コールと同じコールで続けます。 （注） このシナリオは、組み込み型のビデオ ブリッジ機能がエンドポイントに存在しない場合に適用できます。	マルチポイント会議デバイスとビデオエンドポイントです。 サポートされているエンドポイントの一覧については、Cisco Prime Collaboration Assurance でサポートされているデバイス」を参照してください。

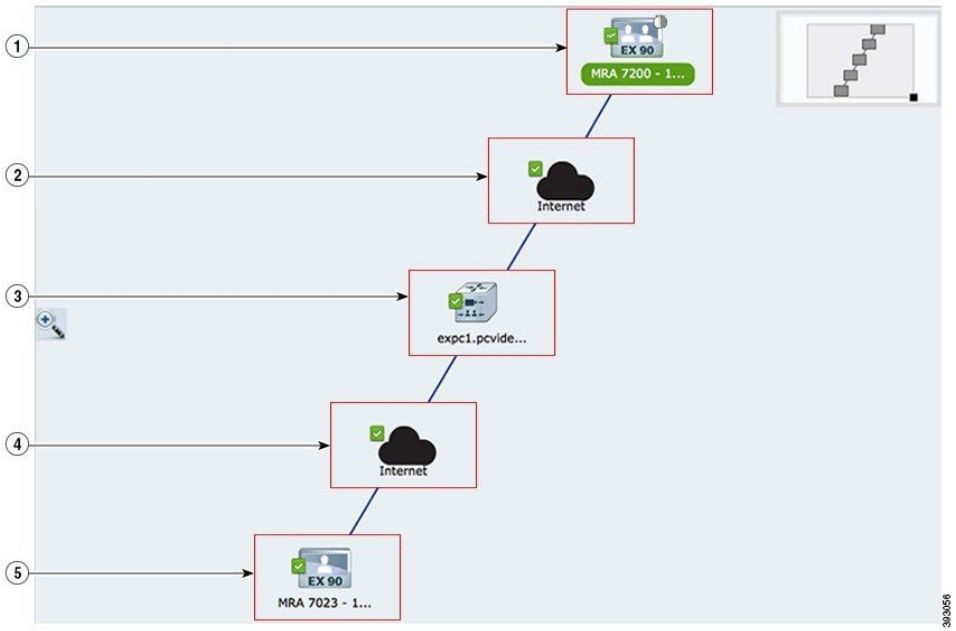
会議の分類	会議タイプ	会議構造	会議トポロジの要素
MRA エンドポイント間の会議： Cisco Jabber、Cisco TelePresence MX シリーズ、Cisco TelePresence System EX シリーズ、または Cisco TelePresence SX シリーズ	アドホック、スケジュール済み	ポイントツーポイント、マルチポイント、マルチサイト （注） Cisco Prime Collaboration Assurance は、MRA エンドポイントが会議ブリッジとして機能しているマルチサイト会議を監視しません。	Cisco Jabber、Cisco TelePresence MX シリーズ、Cisco TelePresence System EX シリーズ、および Cisco TelePresence SX シリーズ。

[1] （Codian ソフトウェアが Cisco MSE で実行されている必要があります）
[2] このシナリオは、CTS 1.7.4、および TC 4.1 から 7.0. をサポートしています。

（注）
- Cisco Jabber デバイスは、アドホック会議のみをサポートします。

次の図には、2 つの MRA エンドポイント間の会議トポロジが示されています。

図 *5 : MRA* エンドポイント間の会議トポロジ



1, 5	クラウド サーバを介して相互に接続されている MRA エンドポイントです。 （注） MRA エンドポイントの会議統計を表示することはできません。
2、4	MRA エンドポイントを接続するインターネット クラウド サーバです。MRA エンドポイントは、クラウド サーバのサポートがある場合のみ接続できます。システムは、クラウド サーバからエンドポイントの IP アドレスを取得できないため、会議統計を表示することはできません。
3	コール コントローラ デバイスとして動作する Cisco VCS Expressway Core です。トポロジには、Cisco VCS Expressway Core と関連付けられたエンドポイントが表示されます。

MRA エンドポイントと VCS Expressway を含む Collaboration Edge のさまざまな会議は、次のとおりです。

- ポイント ツー ポイント：クラウド サーバと Cisco VCS Expressway Core を介して相互に接続されている 2 つの MRA エンドポイント間の会議です
- マルチポイント：クラウド サーバ、Cisco VCS Expressway Core、TPS または MCU を介して接続されている 2 つ以上の MRA エンドポイントがある会議です
- マルチサイト：TPS または MCU なしで接続されている 2 つ以上の MRA エンドポイントがある会議です

（注） 上記の各会議には、いずれかに 1 つの非 MRA エンドポイントがある場合もあります。

表 *51 : MSP* モードの会議シナリオ

会議の分類	会議タイプ	会議構造	会議トポロジの要素
NAT 環境でのお客様によるコールです。	アドホック	ポイント ツー ポイント	Conference Border Controller（SBC）およびビデオエンドポイントです。 サポートされているエンドポイントの一覧については、Cisco Prime Collaboration Assurance でサポートされているデバイス」を参照してください。

会議の診断ダッシュボード

[会議の診断（Conference Diagnostic）] ダッシュボードにアクセスするには、以下を選択します。 **[診断（Diagnose）]** > **[会議の診断（Conference Diagnostics）]**。

[会議の診断（Conference Diagnostic）] ダッシュボードには、会議とその会議に関連するエンドポイントの詳細が表示されます。

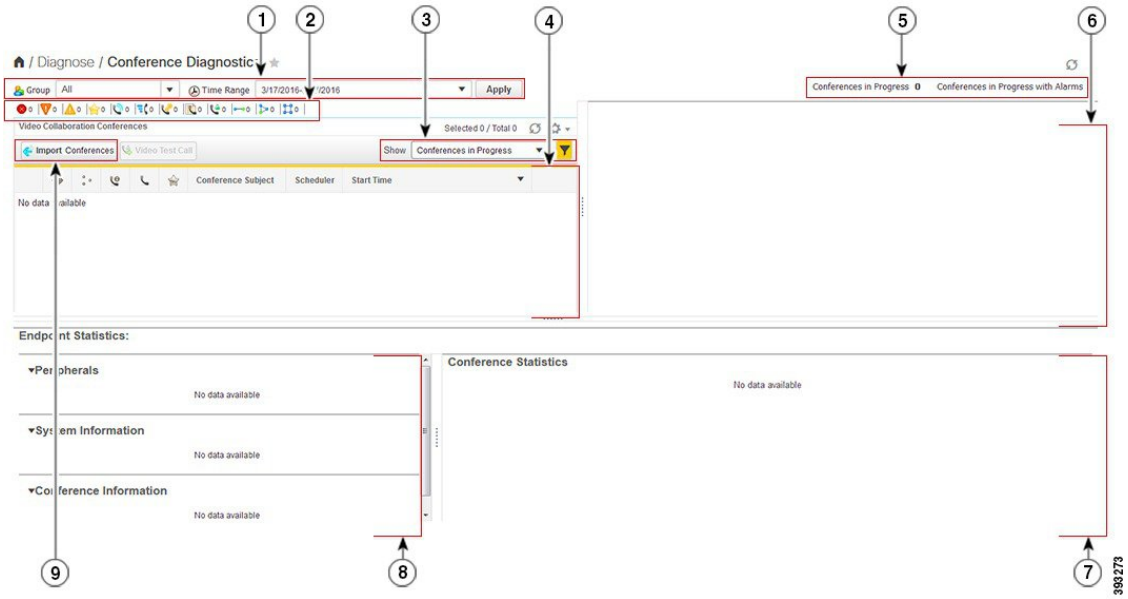
[Group（グループ）] ドロップダウン フィルタから目的のグループを選択することで、デバイス タイプに基づいて会議を監視できます。[Video Collaboration Conferences（ビデオ コラボレーション会議）] ペインの [表示（Show）] フィルタを使用すると、会議タイプに基づき、さらにフィルタをかけることができます。

デフォルトでは、[Video Collaboration Conferences] テーブルには、現在の日付（24 時間）の情報がすべて含まれます。[会議のインポート（Import Conferences）] ボタンの上にマウスのカーソルを合わせると、最後に Cisco Prime Collaboration Assurance データベースにインポートされたデータの詳細時間が表示されます。

（注） Cisco Prime Collaboration Assurance の会議の診断機能は、共有されたディレクトリ番号が設定されている電話機はサポートしません。

次の画像には、会議の診断ダッシュボードが示されています。

図 *6 :* 会議の診断ダッシュボード



1	事前定義された [Group] フィルタのドロップダウンリスト。カレンダーの起動ポイントも含まれています。デフォルトでは、[Video Collaboration Conferences] テーブルには、現在の日付（24 時間）の情報がすべて含まれます。 過去 30 日間と次の 3 日間の会議を表示できます。	2	アラームと会議のクイック サマリー ペインです。

3	事前定義されたフィルタのドロップダウンリスト。 また、[Refresh] アイコンと [Table setting] アイコンもあります。[テーブル（Table）] 設定アイコンを使用してテーブルの列をカスタマイズし、上位または下位のいずれかに固定することができます。	4	ビデオコラボレーション会議
5	進行中の会議（ノーマルまたはアラーム）の総数と、指定日のアラーム付き進行中会議の総数です。	6	会議トポロジのペインです。
7	会議統計のペインです。	8	エンドポイント統計のペインです。このペインには、周辺機器、システム、会議に関する詳細が表示されます。
9	会議のインポートタスクの起動ポイントです。[会議のインポート（Import Conferences）] ボタンの上にマウスのカーソルを合わせると、最後に Cisco Prime Collaboration Assurance データベースにインポートされたデータの詳細時間が表示されます。		

概要ペインには、現在の日付（00:00:00 時から 23:59:00 時）の会議の詳細が表示されます。[Video Collaboration Conferences] テーブルで入手可能なデータのアイコン ベースの概要を表示できます。Cisco Unified IP 電話 8941 および 8945、Cisco DX シリーズ、Cisco TelePresence TX シリーズの DSCP 値を表示できます。作前述のエンドポイントで、会議（**[診断（Diagnose）]**> **[会議の診断（Conference Diagnostics）]**の順に選択）を選択します。[会議統計（Session

Statistics）] ペインの DSCP In フィールドには、会議のエンドポイントから受信した DSCP 値が表示されます。

[ビデオ コラボレーション会議（Video Collaboration Conferences）] テーブルには、現在の日付（00:00:00 から 23:59:59）において進行中の会議の詳細が表示されます。最も新しい会議の詳細がテーブルの先頭にリストされます。

前日または翌日の詳細を表示するには、カレンダーを使用して日付を選択します。[表示（Show）] ドロップダウン リストから任意のフィルタを選択して、他の会議の詳細を表示できます。

Cisco Prime Collaboration Assurance は、過去 30 日に行われた会議の詳細を保持します。

（注） CUCM クラスタ、CUCM ノード、VCS またはビデオエンドポイントを削除した場合、エンドポイントに関連付けられた過去および進行中のすべての会議が削除されます。そのため、関連付けられているセッションは、[会議の診断（Conference Diagnostics）] ページには表示されません。

[会議の診断（Conference Diagnostics）] ダッシュボードには、ビデオ コラボレーション会議以外にも、IP フォン またはソフトウェア クライアントと TelePresence スエンドポイント間の会議が表示されます。これらのデバイスの可視性設定が、[Full Visibility] に設定されていることを確認します。可視性の詳細については、エンドポイントのリアルタイム可視性を参照してください。

Cisco Prime Collaboration Assurance を MSP モードで導入した場合は、会議のデバイスとして MCU を選択し、コールを TMS でスケジュール設定すると、進行中の会議はアドホック会議として表示されます。

Cisco Prime Collaboration Assurance を MSP モードで導入した場合は、セッション ボーダー コントローラを使用して、（異なる Unified CM に登録されている電話機を介して）2 人の顧客間のポイント ツー ポイント コールの詳細を確認できます。そのようなコールの詳細を取得するには、[インベントリ管理（Inventory Management）] でセッション ボーダー コントローラが管理されている状態であることを確認します。

新しい会議方法のサポート：アドホック コール

この機能は、次の [会議の診断（Conference Diagnostics）] ページで、新しいアドホック会議のコールの監視を提供します。**[診断（Diagnose）] > [会議の診断（Conference Diagnostics）]**。

前提条件：Cisco Prime Collaboration Assurance で、マルチポイント コントロール ユニット（MCU）とエンドポイントが Managed 状態である必要があります。

会議ボタンを押してコールが会議モードになった場合、または別のコールとマージした場合、そのコールはマルチポイントのアドホック コールになります。Cisco Unified CM は、コール用の会議デバイスとして動作する MCU を割り当てます。この場合、会議トポロジに MCU が表示されます。最初の参加者がコールから離れると、2 番目と 3 番目の参加者は同じコールを継続し、ポイント ツー ポイントのアドホック コールになります。この場合、会議トポロジに MCU は表示されません。

マルチポイント コントロール ユニット（MCU）が Cisco Prime Collaboration Assurance で Suspended 状態にあり、会議が作成されると、Cisco Prime Collaboration Assurance では 1 つのアドホック コールではなく 2 つのポイント ツー ポイント コールが表示され、エンドポイントとマルチポイント コントロール ユニット（MCU）の間には 2 つ目のコール区間が発生します。数分後にコールは、コールをトリガーしたエンドポイントとマルチポイント コントロール ユニット（MCU）の間で接続されます。トポロジにその他のエンドポイントは表示されません。このシナリオは、組み込み型のビデオブリッジ機能がエンドポイントに存在しない場合に適用できます。

Cisco Unified Communications Manager の監視：Cisco TelePresence Conductor 統合会議

この機能を使用すると、Cisco TelePresence Conductor が統合された Cisco Unified CM によって作成された会議を監視できます。

前提条件：

- Cisco TelePresence Conductor と マルチポイント コントロール ユニット（MCU）は、Cisco Prime Collaboration Assurance で Managed 状態となっている必要があります。
- Cisco TelePresence Conductor の会議ブリッジは、コンダクタの論理検出の一部として検出される必要があります。[デバイスの追加（Add Device）] または [インポート（Import）] 機能を使用して Cisco TelePresence Conductor を検出する場合は、[論理検出を有効にする（Enable Logical Discovery）] のチェックボックスをオンにし、[再検出（Rediscover）] 機能を使用して以降の再検出を実行します。
- Cisco Unified CM を設定し、Cisco TelePresence Conductor を使用してアドホックおよびランデブ会議のための会議ブリッジ リソースを管理します。詳細については、『Cisco TelePresence Conductor with Cisco Unified CM 導入ガイド（XC2.3）』参照してください。

（注） 論理検出は、MSP モードではサポートされていません。

マルチポイント コントロール ユニット（MCU）などの会議デバイスを使用したコールでは、関連付けられたコンダクタの詳細を、会議の診断（[診断（Diagnose）]、[会議の診断（Conference Diagnostics）] の順に移動）ページの [会議（Conference）] トポロジ ペインで、会議デバイス（MCU）にある [エンドポイントのクイック ビュー（Endpoints Quick View）] から確認できます。**[診断（Diagnose）] > [会議の診断（Conference Diagnostics）]**。

Cisco TelePresence Server のカスケード

この機能を使用すると、次の [会議診断（Conference Diagnostics）] ページでアドホック会議のコール中に Cisco TelePresence Server を監視できます。**[診断（Diagnose）] > [会議の診断（Conference Diagnostics）]**。

前提条件 -

- The Cisco TelePresence Server（TPS）、Cisco TelePresence Conductor、およびエンドポイントは、Cisco Prime Collaboration Assurance で Managed 状態となっている必要があります。

• デバイスの可視性設定が、[Full Visibility] に設定されていることを確認します。

アドホック会議中に、プライマリ TPS サーバが Cisco TelePresence Conductor のコールに応答できない場合、そのコールはセカンダリ TPS サーバにカスケードされます。カスケードは、複数の TPS サーバが会議のコール中に負荷を共有する場合に発生します。会議トポロジは、プライマリ TPS サーバとセカンダリ TPS サーバの間に関連付けられた参加者との間でリンクを作成し、すべてのカスケードされた TPS サーバを会議ブリッジとして表示します。

（注） 会議のトラブルシューティングは、Cisco Prime Collaboration Assurance ではサポートされていません。

エンドポイントのリアルタイム可視性

管理されたエンドポイントの可視性機能は、Cisco Prime Collaboration Assurance がエンドポイントの操作をどのレベルで監視するのか決定します。可視性に応じて編集できるのは、[Managed] 状態のエンドポイントのみです。最大レベルの可視性を超えるエンドポイントの可視性設定を編集すると、変更は更新されません。可視性設定は、会議の監視以外にもエンドポイントのポーリングを制御します。ポーリングは、すべてのデバイスではなく、リアルタイムの完全な可視性が設定されているデバイスのみに実行されます。

Cisco Prime Collaboration Assurance は、次のタイプの可視性をサポートします。

• **Full Visibility** - JTAPI/HTTP フィードバックを使用したコール検出、会議統計などのリアルタイムの監視情報、会議情報がサポートされています。

（注） 次の表に一覧化されているエンドポイント統計は、サポートされていません。

1. Cisco Jabber Video for TelePresence (Movi)
2. MRA Endpoints

• Off - JTAPI/HTTP フィードバックを使用したコール検出とリアルタイムの監視情報はサポートされていません。これらのエンドポイントは、淡色表示されたアイコンで [会議監視（Conference Monitoring）] ページに表示されます。

次の表には、エンドポイントのデフォルトおよび最大の可視性に関する詳細が示されています。

エンドポイント タイプ	デフォルトの可視性	最大の可視性
• CTS 500、1000、および 3000 シリーズ • Cisco Codec • Cisco TelePresence SX20 • Cisco TelePresence MXP シリーズ • Cisco IP Video Phone E20	全二重	全二重
• Cisco Jabber Video for TelePresence（Movi）	全二重	全二重
Cisco IP 電話（89xx、99xx）	オフ	全二重
Cisco Desktop Collaboration Experience DX650 および DX630	オフ	全二重
• Cisco SX80 および Cisco SX10 • • Cisco MX200 G2、Cisco MX300 G2、Cisco MX700、および Cisco MX800	全二重	全二重
Cisco DX70 および DX80	オフ	全二重
Cisco Prime Collaboration リリース 11.6 以降の場合 Cisco TelePresence DX70 および DX80	オフ	全二重
MRA エンドポイント： • Cisco Jabber • Cisco TelePresence MX シリーズ • Cisco TelePresence System EX シリーズ • Cisco TelePresence System SX シリーズ	全二重	全二重

エンドポイントの総数には完全な可視性（デフォルトと最大）があります。デフォルトでは、IP フォンやソフトウェア クライアントに可視性はありません。IP フォンおよびソフトウェア クライアントの最大可視性はフルになっています。

ポイント ツー ポイントのアドホック会議では、一方のエンドポイントが [Off] でもう一方が [Full] の場合、可視性が [Off] のエンドポイントは、会議トポロジでは淡色のアイコンで表示されます。

マルチポイント鍵、可視性が [Off] のエンドポイントは会議トポロジに表示されません。

スケジュールされたポイント ツー ポイント会議またはマルチポイント会議の場合、可視性が [Off] のエンドポイントは、会議トポロジでは淡色のアイコンで表示されます。

エンドポイントの可視性を変更するには、**[インベントリ（Inventory）]** > **[インベントリ管理（Inventory Management）]** の順に選択し、対応するエンドポイントのインベントリ テーブルで可視性列を表示します。

（注） この列を表示できない場合は、[設定（Settings）] ボタン、**[列（Columns）]** の順にクリックし、表示される一覧で **[可視性（Visibility）]** をクリックします。

エンドポイントの可視性を変更するには、**[インベントリ（Inventory）]** > **[インベントリ管理（Inventory Management）]** の順にクリックしてエンドポイントを択し、**[編集（Edit）]** をクリック します。エンドポイントの現在の可視性が表示されます。何らかの変更を加えた場合は、**[保存（Save）]** をクリックします。

（注） 複数のエンドポイントを選択した場合、エンドポイントの現在の可視性を表示することはできません。

可視性設定を変更した場合は、次回の会議から実装されます。

可視性機能は、[会議の診断（Conference Diagnostics）] ページのみに適用されます。つまり、可視性を [Off] に設定した場合でも、エンドポイントは [エンドポイントの診断（Endpoint Diagnostics）] および [デバイス インベントリ（Device Inventory）] ページに一覧表示されます。

制限事項

1. 会議の診断機能は、Cisco Unified Communications Manager で複数の回線を使用して設定されたエンドポイントはサポートしません。ただし、これらのエンドポイントは、Cisco Prime Collaboration Assurance インベントリ データベースで管理することができます。
2. Cisco Prime Collaboration Assurance の会議の診断機能は、共有されたディレクトリ番号が設定されている電話機はサポートしません。
3. 会議数が、プロファイルに設定されている最大値を超えることはできません。詳細については、「Cisco Prime Collaboration Assurance のシステム容量」 を参照してください。

4. セッションのモニタリングは、引き続きセキュリティで保護されていない JTAPI 通信を使用し、UCM Mixed モードでセッションを監視します。
5. デバイスの可視性を 「[Full Visibility]」 状態に設定します。
6. Cisco Prime Collaboration Assurance では、会議が前回の Cisco TMS のポーリング後、ならびに次回のスケジュール設定またはオンデマンドによる Cisco TMS のポーリングが発生する前にスケジュール設定され、進行中とされた場合、スケジュール済み会議（ポイントツーポイント、マルチポイント、またはマルチサイト）をアドホック 会議として表示します。
7. いくつかのコール シナリオはサポートされていません。詳細については、会議のワークフローとシナリオセクションを参照してください。

360° 会議ビュー

[360° 会議ビュー（360° Conference View）] は、エンドポイント、インフラストラクチャ デバイス、アラーム、コール レコードに関連するデータの完全なビューを提供します。また、Cisco Prime Collaboration Assurance の他の機能をクロス起動することもできます。会議で [360° 会議ビュー（360° conference View）] を表示するには、[ビデオ コラボレーション会議（Video Collaboration Conferences）] テーブルの [会議の主題（Conference Subject）] 列にマウス ポイントを合わせて、[360 ° 会議ビュー（360° Conference View）] アイコンをクリックします。

[360° 会議ビュー（360° Conference View）] には、次のタブがあります。

- アラーム：アラームの重大度、アラームをトリガーしたソース、生成されたアラームの説明、タイム スタンプが表示されます。
- エンドポイント：エンドポイント名、IPアドレス、物理的な場所、会議の長さ、デバイスモデルが表示されます。
- [インフラストラクチャ（Infrastructure）] : 使用中のインフラストラクチャ デバイスの詳細が表示されます。IP アドレスのリンクを使用すると、[インフラストラクチャデバイス（Infrastructure Devices）] ログイン ページを開くことができます。[デバイス インベントリ（インベントリ）]ページを起動して[デバイス名（Device Name）] をクリックすると、デバイスのインベントリ詳細を表示することもできます。

[360° 会議ビュー（360° Conference View）] では、次の操作を実行できます。

- [アラームの表示（See Alarms）] アイコンをクリックすると、アラーム ブラウザが開きます。Alarm ブラウザには、選択した会議のアラームがすべて（会議とエンドポイント アラームの両方を含む）一覧表示されます。
- [エンドポイントのモニタ（Monitor Endpoint）] アイコンをクリックすると、[エンドポイントの診断（Endpoint Diagnostics）] ページが開きます。
- [ウォッチ リストに追加（Add to Watch）] アイコンをクリックして、ウォッチリストに会議を追加します。これは、スケジュール設定されたおよび進行中の会議で有効になっています。

- 定期的な会議をスケジュール設定している場合は、定期的な会議の各インスタンスをウォッチリストに追加します。たとえば、5 日以上の間で定期的に開催される会議をスケジュール設定した場合、その会議を毎日（5 日）のウォッチリストに追加します。

（注） 会議をウォッチリストに追加しても、トラブルシューティングのワークフローはトリガーされません。

会議トポロジ

会議トポロジには、会議の一部であるエンドポイントが表示されます。マルチポイント会議の場合は、エンドポイントとともに会議デバイスが表示されます。また、コールがトラバーサルコールの場合は、Cisco VCS が表示されます。

会議トポロジを起動するには、[ビデオコラボレーション会議（Video Collaboration Conferences）] テーブルで会議を選択します。

リンクとエンドポイントに表示されるアラームバッジは、それぞれのパケットと周辺機器には障害が発生していることを表します。

次の図には、会議トポロジに表示されるさまざまなステータスが示されています。

図 *7:* セッション トポロジ

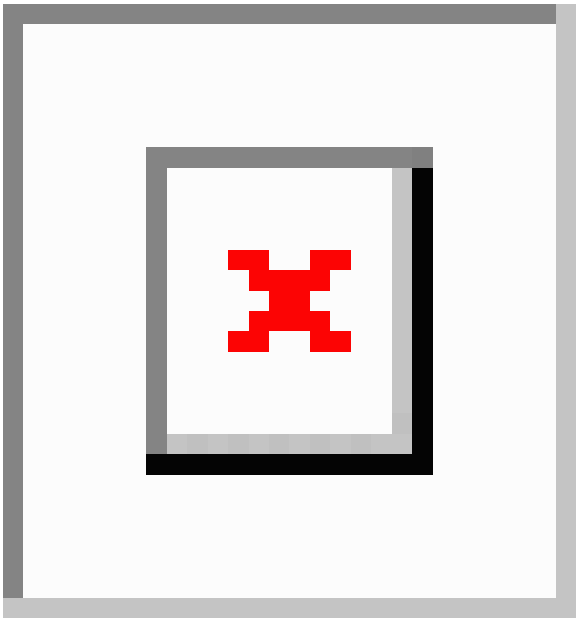


表 *52 :*

ケース	説明	番号（**Number**）	説明
1	エンドポイントに関連付けられた [No-Show] アイコン。	2	アラームなしのエンドポイントとマルチポイントスイッチ間のアクティブなリンクです。
3	そのセッションに参加している、重大なアラームがあるエンドポイントです。ペリフェラルデバイスに問題があります。	4	メジャーなアラームが付いたエンドポイントとマルチポイント スイッチ間のアクティブなリンクです。

ケース	説明	番号（Number）	説明
5	エンドポイントに関連付けられた [Disconnect] アイコンです。	6	不明なエンドポイント：現時点では Cisco Prime Collaboration Assurance で管理されていないエンドポイントです。これらのエンドポイントのインベントリに関する詳細は、Cisco Prime Collaboration Assurance データベースにない場合があります。エンドポイントとコントローラが Managed 状態であり、登録状態が [デバイス 360°（Device 360°）] ビューで利用できる必要があります。 Cisco VCS Expressway に登録されたエンドポイントは、不明なエンドポイントとして表示されます。 Cisco Prime Collaboration Assurance で管理されたエンドポイントは、サポートされていないエンドポイントにコールすることができます。

ネットワークに障害がある場合、アラーム表示はネットワーク ライン上に表示されます。トポロジ上でクイック ビューを起動すると、障害が発生した場所のネットワーク リンクの方向を識別することができます。

ネットワーク リンク クイック ビュー

クイック ビューを起動するには、マウス ポインタをアラーム バッジの上に置き、[クイック ビュー（Quick View）] アイコンをクリックします。ネットワーク リンクのクイック ビューには、次のタブがあります。

- リンクの概要：ポイント ツー ポイント会議用のエンドポイント間や、マルチポイント会議用のエンドポイントとマルチポイント スイッチ間のアラーム ステータスが表示されます。
- アラームの概要：アラームの重大度、アラームをトリガーしたソース、生成されたアラームの説明が表示されます。
- コールの詳細：エンドポイント名、電話番号、およびプロトコルが表示されます。これらの詳細情報は、選択されたネットワーク リンクを介して接続されたエンドポイントに対して表示されます。

エンドポイントのクイック ビュー

エンドポイントのクイック ビューは、Managed および Unknown 状態で起動できます。クイック ビューを起動するには、マウス ポインタをエンドポイントの上に置き、[クイック ビュー（Quick View）] アイコンをクリックします。

[Managed] 状態のデバイスでは、次の詳細が表示されます。

- エンドポイントの概要：システム タイプ、IP アドレス（IPv4 または IPv6）、物理的位置、使用ステータス、ディレクトリ番号（SIP URI または H323 ID）、クラスタ ID など、エンドポイントの詳細が表示されます。

  Cisco Prime Collaboration Assurance を MSP モードで導入した場合は、エンドポイントに属するお客様や、それぞれのプライベート IP アドレスやパブリック IP アドレスを表示することができます。パブリック IP アドレスをクリックすると、エンドポイントの管理アプリケーションを起動できます。
- アラームの概要：アラームの重大度、アラームのカテゴリ、および生成されたアラームの説明が表示されます。

クイック ビューでは、エンドポイントをウォッチリストに追加、エンドポイントの診断ページを起動、ならびに選択したエンドポイントのアラームを表示することができます。

会議リソース：Cisco Prime Collaboration Assurance では、MCU が属する地域に関する情報を表示することができます。

エンドポイント統計

このペインで、エンドポイントの Quality of Service（QoS）をモニタリングできます。実行中のセッションと過去の会議について、エンドポイント統計が表示されます。また、スケジュール済み会議については、周辺機器のステータスとシステム情報が表示されます。

このページには、会議トポロジペインで選択したエンドポイントの周辺機器ステータス、エンドポイント システムの詳細、会議の詳細および統計に関する情報が表示されます。

マルチサイト会議では、センターエンドポイント（会議デバイス）を選択すると、接続する各エンドポイントの会議統計（音声とビデオ）および会議情報が表示されます。

（注） 会議統計の詳細（現在および過去）には、 および Cisco IP 電話については表示されません。

[会議統計（Conference Statistics）]

[会議統計（Conference Statistics）]ペインには、次の項目に対してのパケット損失、遅延、ジッターなどの統計情報が表示されます。

- 音声 — プライマリ コーデック、セカンダリ コーデック 1 と 2、AUX およびプライマリ レガシー。
- ビデオ — プライマリ コーデック、セカンダリ コーデック 1 と 2。

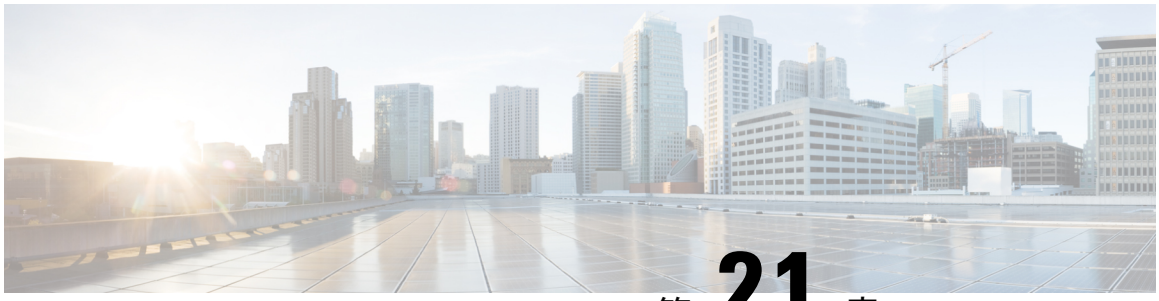
表示される情報は、選択したエンドポイントのタイプによって異なります。

黒の縦線はしきい値を示します。Rx パケット損失、平均周期ジッター、および平均期間遅延のしきい値は、次の値を使用して定義できます。**[アラームおよびレポート管理（Alarm & Report Administration）]**>**[イベントのカスタマイズ（Event Customization）]**>**[しきい値ルール（Threshold Rules）]** オプションが表示されます。

赤は、値が定義されたしきい値を超えたことを示します。グレーは現在の値です。この色はしきい値を持たないパラメータに使用されます。

アラーム表示はネットワーク内の実際の障害を示します。過去の会議に対して、Cisco Prime Collaboration Assurance にしきい値やアラーム バッジ イン 会議統計が表示されることはありません。

1 日以上経過したすべての会議統計とエンドポイント統計データはパージされます。



第 21 章

Cisco APIC-EM を有効にして会議をトラブルシュート

このセクションでは、次の点について説明します。

• Cisco APIC-EM を有効にして会議をトラブルシュート （341 ページ）

Cisco APIC-EM を有効にして会議をトラブルシュート

この章では、Cisco APIC-EM を有効にして会議をトラブルシュートする方法について説明します。

Cisco APIC-EM の概要

Cisco Prime Collaboration リリース 11.6 以降の場合

Cisco Application Policy Infrastructure Controller Enterprise Module （APIC EM）では、ポリシーベースのアプリケーションプロファイルを一元的に自動化することができます。Cisco APIC-EM は既存のネットワーク インフラストラクチャと連携し、ネットワーク全体にわたるネットワーク ポリシーの導入と準拠に関する確認作業を自動化します。詳細については、「Cisco Application Policy Infrastructure Controller Enterprise Module」を参照してください。ネットワークに Cisco APIC EM を導入する際の詳細については、『Cisco Application Policy Infrastructure Controller Enterprise Module 導入ガイド』を参照してください。

Cisco Prime Collaboration Assurance は Cisco APIC と統合し、進行中の音声またはビデオ会議のメディア パスを追跡および監視し、メディア パスの品質を低下させる原因となるネットワーク要素を自動的にトラブルシュートします。

Cisco APIC-EM の主な機能は、次のとおりです。

- ミッドポイントまたは企業ネットワーク デバイス（ルータ、スイッチ、ホスト）を監視し、メディア パスのトラブルシューティングを行います。
- Cisco Prime Collaboration Assurance から受信した 5 タプル（発信元 IP アドレス、宛先アドレス、発信元ポート、宛先ポート、プロトコル）に基づき、パス トレースを実行します。

（注） パス トレースとその制限事項の詳細については、『Cisco Application Policy Infrastructure Controller Enterprise Module 設定ガイド』の「パストレースの実行」セクションを参照してください。

- デバイスを管理するには、SNMP および CLI の両方のクレデンシャルが必要です。
- 特定のフローに対して、メディアパスやパス統計情報（デバイス統計、インターフェイス統計、PerfMon統計）を直接 Cisco Prime Collaboration Assurance に提供します。
- 特定のフローがメディア フローの統計をフェッチするため、ミッドポイントでオンデマンドの PerfMon 設定を行います。会議のトラブルシューティングが終了すると、PerfMon 設定は削除されます。

（注） PerfMonデータが収集可能なプラットフォームの詳細については、http://apic-em/wiki/Category:Testing/Platform_Support#APIC-EM_PLATFORM_SUPPORTの Wiki ページを参照してください。

- 不明な状態にある宛先エンドポイントで、パスのトラブルシューティングを有効にします。

（注）
- Cisco Prime Collaboration Assurance 11.5 Service Pack 1 は、11.5 リリースからのみアップグレードできます。

Cisco APIC-EM コントローラ統合の設定

Cisco Prime Collaboration Assurance では、[Cisco APIC-EMコントローラインテグレーションの設定（Cisco APIC-EM Controller Integration Settings）] を使用して、次に示すようにメディア会議の品質の問題をトラブルシュートできます。 **[アラームおよびレポートの管理（Alarm & Report Administration）]** > **[APIC-EM & Prime のインテグレーション（APIC-EM & Prime Integration）]**。

始める前に

Cisco APIC-EM のロール ROLE_POLICY_ADMIN にユーザが割り当てられていることを確認します。

ステップ 1 選択 **[アラームおよびレポートの管理（Alarm & Report Administration）]** > **[APIC-EM & Prime のインテグレーション（APIC-EM & Prime Integration）]**。

ステップ 2 [APIC-EMコントローラのインテグレーションの設定（APIC-EM Controller Integration Settings）] ペインに有効な Cisco APIC-EM クレデンシャルを入力し、[保存（Save）] をクリックします。

a) Cisco APIC-EM API が入力されたクレデンシャルでアクセスできる場合、Cisco Prime Collaboration Assurance はデータベースに設定の詳細を保存し、ポップアップ メッセージを表示します。

```
APIC-EM credentials are saved successfully.
```

b) Cisco APIC-EM API が入力されたログイン格情報を使用してアクセスできない場合、Cisco Prime Collaboration Assurance は警告メッセージを表示します。

```
APIC-EM is not accessible with the credentials provided. Please verify the
credentials and try again.
```

ステップ 3 [リセット（Reset）] をクリックすると、[APIC-EMコントローラインテグレーションの設定（APIC-EM Controller Integration Settings）] にある Cisco APIC-EM 設定の詳細がクリアされます。

（注） Cisco APIC-EM バージョン 1.2.x は、Cisco Prime Collaboration Assurance リリース 11.5 Service Pack 1 で検証済みです。

Cisco APIC-EM Controller Integration Settings Pane：フィールドの説明

表 *53 : Cisco APIC-EM Controller Integration Settings Pane* のフィールドの説明

フィールド	説明
[IPアドレス（IP Address）]	クラスタの Cisco APIC-EM Controller Management IP アドレスです。到達可能なホスト IP アドレスまたは APIC-EM クラスタの仮想 IP アドレスを入力します。
[HTTP Username] と [Password]	Cisco APIC-EM サーバのログイン クレデンシャルです。

トラブルシューティング

問題 ：テスト接続に失敗しました。

推奨事項：

- **[APIC-EM Controller Integration Settings Pane]** のフィールドにあるクレデンシャルを使用して、Cisco APIC-EM API がアクセスできることを確認します。
- ROLE_POLICY_ADMIN ロールが割り当てられていることを確認します。

Cisco APIC-EM を使用した会議のトラブルシューティング

次の手順には、会議のトラブルシュートを行うための高レベルな手順が含まれています。

始める前に

Cisco Prime Collaboration Assurance が Cisco APIC-EM に統合されていることを確認します。詳細については、Cisco APIC-EM コントローラ統合の設定 （342 ページ）を参照してください。

ステップ 1 Cisco Prime Collaboration Assurance は、指定されたコール区間のエンドポイントから受信した 5 要素の情報を提供することによって、SDN パスのトレースを開始します。

Cisco APIC-EM は、要求を追跡するためのフローを作成します。

ステップ 2 Cisco Prime Collaboration Assurance は、このフローを使用して、メディア パスとパス統計情報を収集します。

Cisco APIC-EM は、指定されたフローのパスに含まれるデバイス（入力または出力インターフェイス）でパフォーマンス モニタの設定を有効にします。トラブルシュートが終了すると、PerfMon の設定が削除されます。

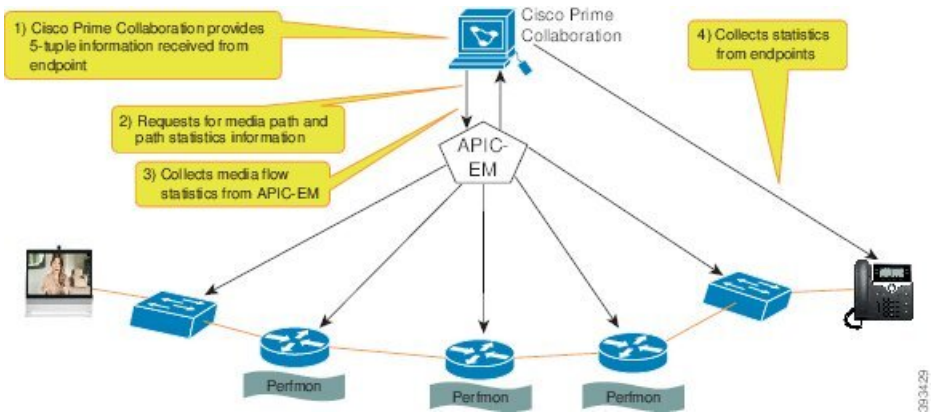
ステップ 3 Cisco Prime Collaboration Assurance は、Cisco APIC-EM コントローラからの各ノードのメディア フローの統計（パケット損失、ジッター、CPU 使用率など）を定期的に収集します。

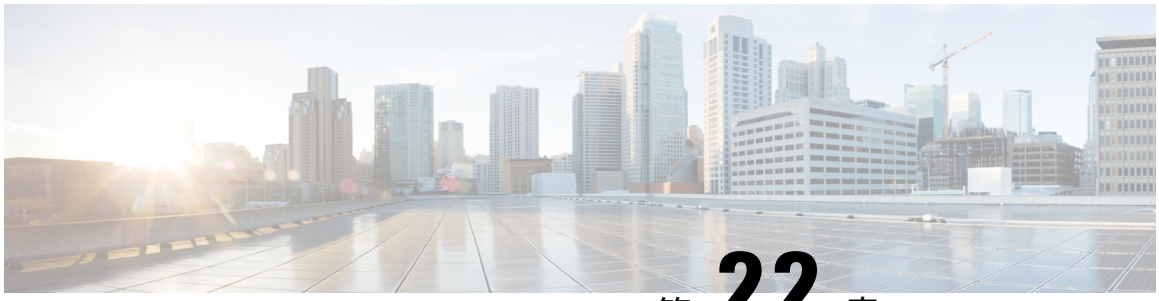
ステップ 4 Cisco Prime Collaboration Assurance は、エンドポイントのポーリングを継続し、エンドポイントからメディア統計を収集します。

例

次の図は、会議のトラブルシュートを行うための、Cisco Prime Collaboration Assurance と Cisco APIC-EM の対話を示しています。

図 *8 : Cisco Prime Collaboration Assurance* と *Cisco APIC-EM* 間の対話





第 22 章

Cisco Prime Collaboration Assurance サーバの監視

このセクションでは、次の点について説明します。

- Cisco Prime Collaboration Assurance サーバの監視 （345 ページ）

Cisco Prime Collaboration Assurance サーバの監視

Cisco Prime Collaboration リリース 11.5 以降の場合

Cisco Prime Collaboration Assurance を使用して、Cisco Prime Collaboration Assurance サーバの正常性を監視できます。CPU、メモリ、ディスク使用率、論理ストレージ領域、プロセスの詳細に関する情報を得ることができます。

前提条件：

- Cisco Prime Collaboration Assurance で SNMP v1、v2c、または v3 を有効にします。SNMP v1、v2c、v3 の有効化に関する詳細については、「Prime Collaboration Assurance 用のデバイスを設定」の「*Configuring Cisco Prime Collaboration Assurance* サーバの設定」セクションを参照してください。
- 管理者のアクセス権を使用して SNMP v1/v2c を有効にします。SNMP v1/v2c を有効にするため、ルート アクセスは必要ありません。
- ルートアクセスを使用して、SNMP v3 を有効にします。ルートアクセスを取得するには、TAC ケースを発生させる必要があります。
- 設定の SNMP v1、v2c、v3 RO またはコミュニティ文字列を使用して、SNMP Manger から Cisco Prime Collaboration Assurance に接続します。

Cisco Prime Collaboration サーバ ヘルスの監視

次の表には、Cisco Prime Collaboration Assurance サーバのヘルスを監視するために必要な MIB の詳細が示されています。

コンポーネント	テーブル	OID	MIB
CPU	systemStats	1.3.6.1.4.1.2021.11	UCD-SNMP-MIB
メモリ	メモリ	1.3.6.1.4.1.2021.4	UCD-SNMP-MIB
ディスク ストレージ	hrDeviceTable	.1.3.6.1.2.1.25.3.2	HOST-RESOURCES-MIB
	hrDiskStorageTable	.1.3.6.1.2.1.25.3.6	
論理ストレージ領域	hrStorageTable	.1.3.6.1.2.1.25.2.3	HOST-RESOURCES-MIB
プロセス	hrSWRunTable	.1.3.6.1.2.1.25.4.2	HOST-RESOURCEs-MIB

例：

- CPU 使用率を監視するには

  SNMP v1 または v2c が有効な場合は、次のコマンドを入力します。

  構文

  # snmpwalk -v2c -c public <PCA IP> UCD-SNMP-MIB::systemStats

  例

  snmptable -v 2c -c public 10.64.91.115 UCD-SNMP-MIB::systemStats

  SNMP v3 が有効な場合は、次のコマンドを入力します。

  構文

  snmpwalk -v 3 -A authpasswd -X privpasswd -x AES -l authPriv -u user1 -a MD5 <PCA IP> UCD-SNMP-MIB::systemStats

  例

  snmpwalk -v 3 -A authpasswd -X privpasswd -x AES -l authPriv -u jane -a MD5 <PCA IP> UCD-SNMP-MIB::systemStats

  出力例

```
UCD-SNMP-MIB::ssIndex.0 = INTEGER: 1
UCD-SNMP-MIB::ssErrorName.0 = STRING: systemStats
UCD-SNMP-MIB::ssSwapIn.0 = INTEGER: 0 kB
UCD-SNMP-MIB::ssSwapOut.0 = INTEGER: 0 kB
UCD-SNMP-MIB::ssIOSent.0 = INTEGER: 609 blocks/s
UCD-SNMP-MIB::ssIOReceive.0 = INTEGER: 0 blocks/s
UCD-SNMP-MIB::ssSysInterrupts.0 = INTEGER: 994 interrupts/s
UCD-SNMP-MIB::ssSysContext.0 = INTEGER: 5508 switches/s
UCD-SNMP-MIB::ssCpuUser.0 = INTEGER: 6
UCD-SNMP-MIB::ssCpuSystem.0 = INTEGER: 0
```

```
UCD-SNMP-MIB::ssCpuIdle.0 = INTEGER: 87
UCD-SNMP-MIB::ssCpuRawUser.0 = Counter32: 15940286
UCD-SNMP-MIB::ssCpuRawNice.0 = Counter32: 14270
UCD-SNMP-MIB::ssCpuRawSystem.0 = Counter32: 1046654
UCD-SNMP-MIB::ssCpuRawIdle.0 = Counter32: 193992466
UCD-SNMP-MIB::ssCpuRawWait.0 = Counter32: 6614683
UCD-SNMP-MIB::ssCpuRawKernel.0 = Counter32: 0
```

- メモリ使用率を監視するには

  SNMP v1 または v2c が有効な場合は、次のコマンドを入力します。

  構文

  # snmpwalk -v2c -c public <PCA IP> UCD-SNMP-MIB::memory

  例

  snmptable -v 2c -c public 10.64.91.115 UCD-SNMP-MIB::memory

  SNMP v3 が有効な場合は、次のコマンドを入力します。

  構文

  snmpwalk -v 3 -A authpasswd -X privpasswd -x AES -l authPriv -u user1 -a MD5 <PCA IP> UCD-SNMP-MIB::memory

  例

  snmpwalk -v 3 -A authpasswd -X privpasswd -x AES -l authPriv -u jane -a MD5 <PCA IP> UCD-SNMP-MIB::memory

  出力例

```
UCD-SNMP-MIB::memIndex.0 = INTEGER: 0
UCD-SNMP-MIB::memErrorName.0 = STRING: swap
UCD-SNMP-MIB::memTotalSwap.0 = INTEGER: 25165816 kB
UCD-SNMP-MIB::memAvailSwap.0 = INTEGER: 25165724 kB
UCD-SNMP-MIB::memTotalReal.0 = INTEGER: 14236500 kB
UCD-SNMP-MIB::memAvailReal.0 = INTEGER: 848220 kB
UCD-SNMP-MIB::memTotalFree.0 = INTEGER: 26013944 kB
UCD-SNMP-MIB::memMinimumSwap.0 = INTEGER: 16000 kB
UCD-SNMP-MIB::memShared.0 = INTEGER: 0 kB
UCD-SNMP-MIB::memBuffer.0 = INTEGER: 516240 kB
UCD-SNMP-MIB::memCached.0 = INTEGER: 3495964 kB
UCD-SNMP-MIB::memSwapError.0 = INTEGER: noError(0)
UCD-SNMP-MIB::memSwapErrorMsg.0 = STRING:
```

- ディスク ストレージの詳細を監視するには

SNMP v1 または v2c が有効な場合は、次のコマンドを入力します。

構文

```
snmptable -v 2c -c public <PCA IP> [OID]
```

例

```
snmptable -v 2c -c public <PCA IP> .1.3.6.1.2.1.25.3.2
```

SNMP v3 が有効な場合は、次のコマンドを入力します。

構文

```
#snmptable -v 3 -A authpassword -X privpassword -x AES -l authPriv
-u user1 <PCA IP> [OID]
```

例

```
#snmptable -v 3 -A authpassword -X privpassword -x AES -l authPriv
-u user1 <PCA IP> .1.3.6.1.2.1.25.3.2
```

出力例

表 *54 : SNMP table: HOST-RESOURCES-MIB::hrDeviceTable*

hrDeviceIndex	hrDeviceDescr	hrDeviceType	hrDeviceID	hrDeviceStatus	hrDeviceErrors
1552	HOST-RESOURCES-TYPES::hrDeviceDiskStorage	SCSI disk (/dev/sda)	SNMPv2-SMI::zeroDotZero	実行	?
1538	HOST-RESOURCES-TYPES::hrDeviceDiskStorage	VMware Virtual IDE CDROM Drive	SNMPv2-SMI::zeroDotZero	実行	?

SNMP v1 または v2c が有効な場合は、次のコマンドを入力します。

構文

```
snmptable -v 2c -c public <PCA IP> [OID]
```

例

```
snmptable -v 2c -c public <PCA IP> .1.3.6.1.2.1.25.3.6
```

SNMP v3 が有効な場合は、次のコマンドを入力します。

構文

```
#snmptable -v 3 -A authpassword -X privpassword -x AES -l authPriv
-u user1 <PCA IP> [OID]
```

例

#snmptable -v 3 -A authpassword -X privpassword -x AES -l authPriv -u user1 <PCA IP> .1.3.6.1.2.1.25.3.6

出力例

表 55 : SNMP table: HOST-RESOURCES-MIB::hrDiskStorageTable

hrDiskStorageAccess	hrDiskStorageMedia	hrDiskStorageRemoveble	hrDiskStorageCapacity
readWrite	unknown	true	0KBytes
readWrite	unknown	false	262144000 KBytes

- 論理ストレージ領域を監視するには

SNMP v1 または v2c が有効な場合は、次のコマンドを入力します。

構文

snmptable -v 2c -c public <PCA IP> [OID]

例

snmptable -v 2c -c public <PCA IP> .1.3.6.1.2.1.25.2.3

SNMP v3 が有効な場合は、次のコマンドを入力します。

構文

#snmptable -v 3 -A authpassword -X privpassword -x AES -l authPriv -u user1 <PCA IP> [OID]

例

#snmptable -v 3 -A authpassword -X privpassword -x AES -l authPriv -u user1 <PCA IP> .1.3.6.1.2.1.25.2.3

出力例

表 56 : SNMP table: HOST-RESOURCES-MIB::hrStorageTable

hrStorageIndex	hrStorageType	hrStorageDescr	hrStorageAllocationUnits	hrStorageSize	hrStorageUsed	hrStorageAllocationFailures
1	HOST-RESOURCES-TYPES::hrStorageRam	物理メモリ	1024 バイト	14236500	13338404	?
3	HOST-RESOURCES-TYPES::hrStorageVirtualMemory	Virtual memory	1024 バイト	39402316	13338496	?

- プロセスの詳細を監視するには

SNMP v1 または v2c が有効な場合は、次のコマンドを入力します。

構文

snmptable -v 2c -c public <PCA IP> [OID]

例

snmptable -v 2c -c public <PCA IP> .1.3.6.1.2.1.25.4.2

SNMP v3 が有効な場合は、次のコマンドを入力します。

構文

#snmptable -v 3 -A authpassword -X privpassword -x AES -l authPriv -u user1 <PCA IP> [OID]

例

#snmptable -v 3 -A authpassword -X privpassword -x AES -l authPriv -u user1 <PCA IP> .1.3.6.1.2.1.25.4.2

出力例

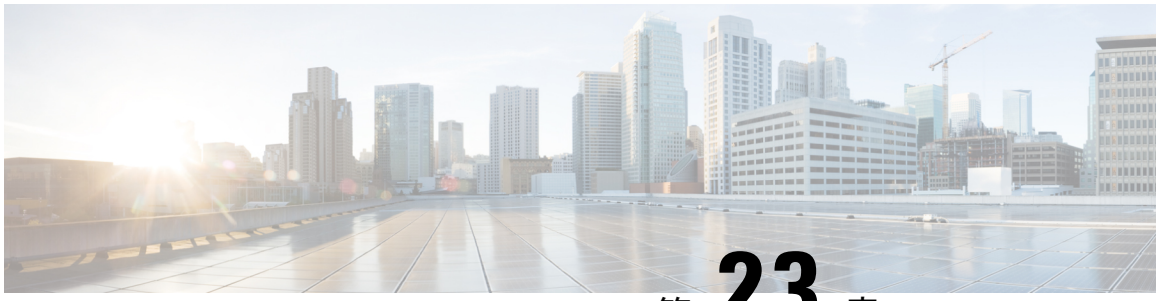
表 *57 : SNMP table: HOST-RESOURCES-MIB::hrSWRunTable*

hrSW RunIndex	hrSW RunName	hrSW RunID	hrSW RunParameters	hrSW RunType	hrSW RunStatus	hrSW Runpath
2367	postgres	SNMPv2-SMI : : zeroDotzero	""	アプリケーション	runnable	postgres: cmuser cpcm 127.0.0.1 (51478) idle
2643	postmaster	SNMPv2-SMI : : zeroDotzero	""	アプリケーション	runnable	postgres: primea cqdb 127.0.0.1 (50175) FETCH

第 VI 部

ダッシュボードとレポート

- Cisco Prime Collaboration Assurance ダッシュボード （353 ページ）
- Cisco Prime Collaboration Assurance レポート （467 ページ）



第 23 章

Cisco Prime Collaboration Assurance ダッシュボード

このセクションでは、次の点について説明します。

• Cisco Prime Collaboration Assurance ダッシュボード （353 ページ）

Cisco Prime Collaboration Assurance ダッシュボード

Cisco Prime Collaboration Assurance ダッシュボードは、デバイス、アプリケーション、エンドポイントに関する情報を統合して提供します。これらのダッシュボードを使用して、次のことができます。

- 1 つのインターフェイスを使用して、ユーザのすべてのエンドポイントを監視します。
- すべてのエンドポイント用のサービス エクスペリエンスを決定します。

  Cisco Prime Collaboration リリース 11.5 以降の場合

  すべてのエンドポイントのコール品質を決定します。

ダッシュボードにデータを追加するには、次のタスクを実行する必要があります。

- デバイスを検出します
- 会議をインポートする（会議関連のダッシュボードの場合）
- デバイスをポーリングする

[Cisco Prime Collaboration Assurance] ページの [ナビゲーションの切り替え（Toggle Navigation）] アイコン をクリックすると、ダッシュレットとレポートのリストが表示されます。左上のピン アイコンをクリックすると、左側のペインの表示/非表示を切り替えることができます。同じメニューで、インデックスを表示したり、お気に入りを設定したり、検索オプションを使用したりすることもできます。

（注） ブラック リボン フレーム上にある Cisco Prime Collaboration Assurance の完全なタイトルを表示するには、コンピュータの画面解像度を変更する必要があります。[インデックス（Index）]の左上のペインにある[トグル（Toggle）]ピンボタンをクリックして、タイトルを表示します。

次の表には、Cisco Prime Collaboration Assurance ダッシュボードの説明が示されています。

ダッシュボード	説明	**Prime Collaboration Assurance の導入**
OpsView（**[監視（Monitor）]> [システム ビュー（System View）]> [OpsView]**）	Cisco Unified CM および VCS クラスタの概要を提供します。	Prime Collaboration Assurance Advanced
サービス エクスペリエンス（**[監視（Monitor）]> [システム ビュー（System View）]> [サービス エクスペリエンス（Service Experience）]**）	セッションおよびアラームに関する情報。	Prime Collaboration Assurance Advanced
アラーム（**[監視（Monitor）]> [システム ビュー（System View）]> [アラーム（Alarm）]**）	管理デバイスに関する情報です。	Prime Collaboration Assurance Advanced
パフォーマンス（**[監視（Monitor）]> [システム ビュー（System View）]> [パフォーマンス（Performance）]**）	各管理対象デバイスの重要なパフォーマンス メトリックについて詳細情報を提供します。	Prime Collaboration Assurance Advanced
Contact Center トポロジ（**[監視（Monitor）]> [システム ビュー（System View）]> [Contact Center トポロジ（Contact Center Topology）]**）	CUIC、Finesse、MediaSense、CVP、UCCE などの Contact Center コンポーネントに関する情報です。	Prime Collaboration Contact Center Assurance
使用率モニタ（**[監視（Monitor）]> [使用率モニタ（Utilization Monitor）]**）	エンドポイントとその使用率、会議デバイス、ライセンスの使用状況に関する情報です。	Prime Collaboration Assurance Advanced

Cisco Prime Collaboration リリース 11.5 以降の場合

ダッシュボード	説明	**Cisco Prime Collaboration Deployment**
OpsView**[ネットワーク正常性の概要（Network Health Overview）] > [OpsView]**）	Cisco Unified CM および VCS クラスタの概要を提供します。	Cisco Prime Collaboration Assurance Advanced
コール品質 **([ネットワーク正常性の概要（Network Health Overview）] > [コール品質（Call Quality）]**）	サービス品質に関する情報です。	Cisco Prime Collaboration Assurance Advanced
アラーム**[ネットワーク正常性の概要（Network Health Overview）] > [アラーム（Alarm）]**）	アラームの概要に関する情報です。	Cisco Prime Collaboration Assurance Advanced
[パフォーマンス（Performance）]**[ネットワーク正常性の概要（Network Health Overview）] > [パフォーマンス（Performance）]**）	各管理対象デバイスの重要なパフォーマンスメトリックについて詳細情報を提供します。	Cisco Prime Collaboration Assurance Advanced
Contact Center トポロジ（**[ネットワーク正常性の概要（Network Health Overview）] > [Contact Center トポロジ（Contact Center Topology）]**）	Unified Contact Center トポロジビューに関する情報です。	Cisco Prime Collaboration Contact Center Assurance

Cisco Prime Collaboration Assurance を MSP モードで導入した場合は、Cisco Prime Collaboration Assurance ホームページから次のダッシュボードを表示できます。

ダッシュボード	説明
顧客の概要（**[監視（Monitor）]> [システム ビュー（System View）]> [顧客の概要（Customer Summary）]**）	カスタマーごとのアラーム、エンドポイント、インベントリに関する情報。

TelePresence Exchange（**[監視（Monitor）]> [システム ビュー（System View）]> [Telepresence Exchange]**）	クラスタ ノード、コールおよびセッション制御デバイス、リージョンの概要、および会議デバイスに関する情報。 （注） CTXデバイスが管理されていない場合、ダッシュレットにデータは追加されません。

Cisco Prime Collaboration リリース 11.5 以降の場合

Cisco Prime Collaboration Assurance を MSP モードで導入した場合は、Cisco Prime Collaboration Assurance ホームページから次のダッシュボードを表示できます。

ダッシュボード	説明
カスタマーサマリ**[ネットワーク正常性の概要（Network Health Overview）] > [カスタマーサマリ（Customer Summary）]**）	カスタマーごとのアラーム、エンドポイント、インベントリに関する情報。
TelePresence Exchange**[ネットワーク正常性の概要（Network Health Overview）] > [TelePresence Exchange]**）	クラスタ ノード、会議の制御デバイス、地域の概要、会議デバイスに関する情報です。

カスタマー サマリ ダッシュボードを使用すると、エンドポイントやインフラストラクチャ デバイスの詳細情報、および特定のカスタマーのネットワークの論理的なトップレベル ビューを確認できます。これにより、前述の表に記載されている、個々の顧客用のその他のダッシュボードが開きます。

（注）

- Cisco Prime Collaboration Assurance の Enterprise ダッシュボード（保持しているライセンスに応じたサービス エクスペリエンス、アラーム、Contact Center トポロジ、使用状況モニタ）は、デフォルトでは、グローバル顧客選択フィールドを介してコンテンツをフィルタリングすることはありません。
- **Cisco Prime Collaboration リリース 11.5 以降の場合**

  Cisco Prime Collaboration Assurance の Enterprise ダッシュボード（保持しているライセンスに応じたコール品質、アラーム、Contact Center トポロジ）は、デフォルトでは、グローバル顧客選択フィールドを介してコンテンツをフィルタリングすることはありません。
- グローバル選択で別の顧客を選択するとユーザインターフェイスが更新され、ホームページには [カスタマー サマリ（Customer Summary）] ダッシュボードが表示されます。
- 顧客を変更するには、[カスタマーサマリ（Customer Summary）] ダッシュボードで顧客名をクリックする必要があります。

データは、チャートまたは表形式で表示できます。デフォルトでは、レポートはインタラクティブなグラフとして表示されます。つまり、データをクリックすると、関連付けられている

ページが起動します。表形式でレポートを表示すると、CSV形式でデータをエクスポートできます。

このダッシュボードでは、次のデータを表示できます。

- 1 日 - 00:00:00 時間から現在の時刻までのデータが収集されます。
- 1 週間 - 00:00:00 時間から開始した、当日を含む過去 7 日間のデータが収集されます。
- 4 週間 - 00:00:00 時間から開始した、当日を含む過去 28 日間のデータが収集されます。

（注） すべてのページで表示される時間は、Cisco Prime Collaboration Assurance サーバの時間です。

Ops View

ホームページの Ops ビューまたはクラスタ ビュー（**[モニタ（Monitor）] > [システム ビュー（System View）] > [OpsView]**）では、システムで使用可能な Cisco Unified CM および VCS クラスタに関する概要レベルの情報を確認できます。導入モードに基づいて、システム内のすべてのクラスタ、または特定の顧客のクラスタについての詳細を表示できます。Ops ビューには、ハード エンドポイントおよびソフト エンドポイントの未登録数が個別のエンティティとして表示されます。

Cisco Prime Collaboration リリース 11.5 以降の場合

Ops ビューまたはクラスタ ビューはホームページに表示されます（**[ネットワーク正常性の概要（Network Health Overview）] > [OpsView]**。

Cisco Prime Collaboration リリース 11.6 以降の場合

また、[Opsビュー（OpsView）] タブには、Unified Communications Manager クラスタに接続されている SIP トランクの詳細も表示されます。

前提条件：

- クラスタ データを Ops ビューに表示するには、クラスタを Cisco Prime Collaboration Assurance で検出する必要があります。
- ユーザは、システム内に 1 つ以上の Cisco Unified CM または VCS クラスタが存在するドメインまたは顧客に関連付けられている必要があります。ただし、globaladmin ユーザはすべてのドメインにアクセスできるため、これには該当しません。
- CUCM の syslog レシーバとして、Cisco Prime Assurance サーバを追加します。これにより、Ops ビューが動的に更新され、クラスタ内のトランク ステータスの変更が反映されます。

（注） Ops ビューに何も表示されていない場合は、『Cisco Prime Collaboration Assurance and Analytics インストールおよびアップグレード ガイド』の「*Prime Collaboration Assurance* を使用する前に」のセクションにある注意事項を参照してください。

クラスタの詳細を参照するには、[ツリーマップ（Treemap）] ビューまたは [リスト（List）] ビューを使用します。

ツリーマップ ビューを使用する場合	リスト ビューを使用する場合
障害の概要と、[深刻（Critical）]、[重大（Major）]、[やや重大（Minor）]、[警告（Warning）] のアラームを分割して表示します。[合計アラーム数（Total alarms count）] リンクをクリックすると、[アラームとイベント（Alarms & Events）] ページで、[アラーム（Alarm）] ブラウザを起動できます。 （注） Ops ビューに表示される合計アラーム数には、クラスタ ノード上で生成されたアラームだけでなく、個々のデバイスで生成されたアラーム（Cisco Unified CM または VCS クラスタに関連付けられている場合）も含まれています。	障害の概要と、[深刻（Critical）]、[重大（Major）]、[やや重大（Minor）]、[警告（Warning）] のアラームを分割して表示します。[合計アラーム数（Total alarms count）] をクリックすると、[アラームとイベント（Alarms & Events）] ページで、[アラーム（Alarm）] ブラウザをブラウザ起動できます。
クラスタ内のすべての異なるタイプのデバイス（電話機、メディア リソース（ハードウェアおよびソフトウェア）、MGCP ゲートウェイ（各ポートを含む）、CTI ルート ポイント、CTI ポート、ボイス メール ポートなど）の登録情報（登録済み、未登録のハード エンドポイントまたはソフトクライアント、バックアップに登録されている、不明のエンドポイント数）が表示されます。 エンドポイントの登録ステータス数をクリックすると、[**エンドポイントの診断（Endpoint Diagnostics）**] ページが起動されます。他のデバイス タイプの登録ステータス数をクリックすると、そのデバイス タイプでフィルタリングされたすべてのデバイスが含まれる [**接続デバイス（Connected Devices）**] タブが起動されます。	各デバイス タイプの登録済み、未登録のハード エンドポイントまたはソフト クライアント、バックアップに登録されている、不明の電話数が表示されます。エンドポイントの電話数をクリックすると、[エンドポイントの診断（Endpoints Diagnostics）] ページが起動されます。他のすべてのデバイス タイプ（メディア リソース、ボイス メール ポート、MGCP ゲートウェイ）の電話数をクリックすると、そのデバイス タイプでフィルタリングされたすべてのデバイスが含まれる [接続デバイス（Connected Devices）] タブが起動されます。 **CTI ポート**と **CTI ルート ポイント**のデバイス タイプはデフォルトで表示されます。

ツリーマップ ビューを使用する場合	リスト ビューを使用する場合
クラスタ名をクリックして、そのクラスタの [概要（Summary）] ビューを起動します。	クラスタ名をクリックして、そのクラスタの [概要（Summary）] ビューを起動します。

（注）

- [ツリーマップ（Treemap）] ビューに表示されるデータは、システムで使用可能なコンポーネントによって異なります。ただし、アラームに関する情報は、すべてのクラスタについて表示されます。
- ツリーマップ ビューまたはリスト ビューで VCS クラスタをクリックすると、[トポロジ（Topology）] ページのみが起動されます。サマリー、デバイス プール別のエンドポイント、接続されたデバイス、ルートパターンの概要、およびデバイス検索タブは、Cisco のユニファイド CM クラスタにのみ適用されます。
- 10 以上のクラスタが導入されている場合は、ツリーマップ ビューに各クラスタのタイトル リンクが表示されます。

ツリーマップ ビューでは、アラームの詳細についてはアラーム コンポーネント、登録ステータス情報についてはデバイス タイプ コンポーネントをクリックすることによって、上記の詳細を簡易ビューで表示することもできます。

ツリーマップ ビューは 2 分ごとに自動で更新されます。自動更新機能を無効にするには、ツリーマップ ビューの右上隅にある [自動更新（Auto Refresh）] チェックボックスをオフにします。

ツリーマップ ビューのカラー コード：

ツリーマップ ビューでは、クラスタ内のデバイス タイプとアラームが次の重大度のカテゴリに基づいて分類されます。

重大度	表示される色	意味
クリティカル	赤	• クラスタ内に 1 つ以上の深刻なアラームがあります。 または • 未登録のハード エンドポイントが 10% 以上あります。 または • **Cisco Prime Collaboration リリース 11.6 以降の場合** 少なくとも 1 つの Unified Communications Manager SIP トランク が 「No Service」 状態です。 （注） 赤色が表示されている時は、Ops ビューにハードおよびソフトの未登録のエンドポイントカウントが個別に表示されます。

重大度	表示される色	意味
メジャー	オレンジ	• クラスタ内に 1 つ以上重大なアラームがあります。 または • 未登録のハード エンドポイントが 10% 未満です。 または • **Cisco Prime Collaboration リリース 11.6 以降の場合** 少なくとも 1 つの Unified Communications Manager SIP トランク が 「Partial Service」 状態であり、「No Service」 状態の Unified Communications Manager SIP トランクはありません。 （注） オレンジ色が表示されている時は、Ops ビューにハードおよびソフトの未登録のエンドポイントカウントが個別に表示されます。

重大度	表示される色	意味
やや重大/警告	黄	• クラスタ内に 1 つ以上のやや重大または警告のアラームがあります。 または • BackUp 状態の登録済みデバイスがあります。 または • **Cisco Prime Collaboration リリース 11.6 以降の場合** 少なくとも 1 つの Unified Communications Manager SIP トランクが「UNKNOWN-Options Ping Enabled」 状態で、「No Service」 状態、「Partial Service」 状態の Unified Communications Manager SIP トランクがありません。

重大度	表示される色	意味
通常	グリーン	• 深刻、重大、やや重大のいずれのアラームもありません。 または • すべてのデバイスが登録済みまたは不明な状態です。 または • **Cisco Prime Collaboration リリース 11.6 以降の場合** 完全なサービス状態のすべての Unified Communications Manager SIP トランクが 「Full Service」 状態です。 または • クラスタに対して、Unified Communications Manager SIP トランクが 1 つも定義されていません。

（注） **Cisco Prime Collaboration リリース 11.6 以降の場合**

Unified Communications Manager クラスタに関連付けられている SIP トランクの場合、リストビューには、以下の状態を表すカラム名が表示されます。

- [サービスなし（No Service）]
- [部分的なサービス（Partial Service）]
- UNKNOWN-Options Ping Enabled
- [完全なサービス（Full Service）]

トラブルシューティング

1. **問題**：Ops ビューにクラスタが表示されない

   推奨処置：次の条件が満たされていることを確認します。

- クラスタが検出されており、Cisco Unified CM がインベントリ管理で管理状態になっている
- クラスタの CDT 検出が完了しており、インベントリ管理に表示されている
- エンドポイントの診断にすべてのエンドポイントが表示されている

2. **問題**：登録ステータスに正しいカウントが表示されない

   推奨処置：次の条件が満たされていることを確認します。

   - CDT 検出によってカウント情報が更新されている
   - CDT 検出が正常に完了していない場合は、CDT の検出をもう一度トリガーする必要がある
   - Cisco Unified CM が有効になっており、syslog が Cisco Prime Collaboration Assurance に送信されている

3. **問題**：UCM SIP トランクのリーフの色が想定どおりに変更されない。

   推奨処置：次の条件が満たされていることを確認します。

   - トランク ステータスの変更は Cisco Prime Collaboration Assurance への syslog 更新として提供されるため、CUCM で Prime Collaboration Assurance が syslog の受信者として追加されているかどうかを確認します。
   - もう 1 つの回避策は、CUCM を再検出することです。

4. **問題**：globaladmin ユーザが [OpsViewダッシュレット（OpsView Dashlets）] ページを表示できないことがある。

   推奨処置：次のスクリプトを実行します。

   新しいスクリプト **opsview_globaladmin.sh** が作成されます。

   推奨されるパス：スクリプトをパス **/opt/emms/emsam/bin** に保存します。

概要（Summary）

[概要（Summary）] タブには、クラスタ内にある各 Unified CM ノードのシステム使用率に関するステータスが表示されます。

次のようなダッシュレットがあります。

- 概要（Summary）
- コール プロセッサの正常性に関する概要
- アラームの概要
- 登録の概要
- ライセンスの概要

概要（Summary）

高レベルなクラスタ情報や、設定済みのH323、MGCPゲートウェイ、SIPトランク、デバイスプールの数など、クラスタ間の詳細を提供します。

また、クラスタバージョン、データベースレプリケーションステータス、クラスタ内のUnified CMノードの数を確認することもできます。クラスタ内にあるUnified CMノードの直近24時間のコールアクティビティグラフを表示するには、**[クラスタ コール アクティビティ（Cluster Call Activity）]**をクリックします。

コール プロセッサの正常性に関する概要

現在の時間とピーク時のCPU使用率、仮想メモリ使用量、ディスク使用量、コールの試行回数または完了数に関する情報を提供します。選択したUnified CMノードで直近24時間のコールアクティビティグラフを表示するには、**[コールvアクティビティ（Call Activity）]**をクリックします。選択したクラスタ タイプで、システムの概要ダッシュボードが付いた[パフォーマンス（Performance）]タブを起動するには、CPU使用率、VM使用率、またはディスク使用率の値をクリックします。

また、Cisco Unified CMクラスタの長期的なコールアクティビティの傾向を表示することもできます。これを表示するには、1つ以上のクラスタ ノード選択し、**[トレンド（Trend）]**のドロップダウン リストから**[コール アクティビティ（Call Activity）]**を選択します。

（注） IM & Presenceに適用されないフィールドは、[N/A]として表示されます。

アラームの概要

Cisco Prime Collaboration Assuranceが管理するすべてのクラスタの不具合で、高レベルな概要を提供します。[合計（Total）]列のアラームデータをクリックすると、[アラームとイベント（Alarms & Events）]ページのAlarmブラウザへとクロス起動できます。

登録の概要

電話機、メディアリソース（ハードウェアとソフトウェア）、MGCPゲートウェイ（各ポートを含む）、CTIルートポイント、CTIポート、クラスタ内の音声メールポートの登録ステータスに関する情報を提供します。

エンドポイントについて、次の情報が表示されます。

- 登録されているエンドポイントの数
- バックアップに登録されているエンドポイントの数
- 未登録エンドポイントの数
- 不明または拒否されたエンドポイント数

上記の登録ステータスでそれぞれのエンドポイントデータをクリックすると、そのデバイスタイプに[接続されているデバイス（Connected Devices）]タブが起動します。

ライセンスの概要

Cisco Unified CM クラスタのライセンス情報を提供します。バージョン 9.0 以降の場合は、**[ここをクリックして CUWL ライセンスの詳細を表示（Click here for CUWL License Details）]** リンクをクリックすると、Cisco Prime License Manager のログイン ページが起動します。

バージョン 9.0 以前の場合は、ライセンス タイプ、認可済みユニット、使用ユニット、残りのユニットなどのライセンス情報を取得して表示します。

デバイス プール別のエンドポイント

[デバイス プール別のエンドポイント（Endpoint by Device Pool）] タブには、デバイス プール レベルでクラスタの電話の概要が示されます。

次の情報を表示します。

- このデバイス プールに設定されたエンドポイントの数
- 登録されているエンドポイントの数
- バックアップに登録されているエンドポイントの数
- 未登録エンドポイントの数
- 不明または拒否された状態のエンドポイント数
- サービス品質のエンドポイントとイベント。

前述のいずれかの登録ステータスのエンドポイント データをクリックすると、[エンドポイントの診断（Endpoint Diagnostics）] ページへの相互起動ができます。

[SQに関する問題（SQ Issues）] 列でエンドポイント データをクリックすると、[影響を受ける電話のレポート（Impacted Phones Report）] ページが開きます。このページには、音声品質の問題によって影響を受けるデバイス プール内のすべての電話が一覧表示されます。

[SQに関する問題（SQ Issues）] 列のイベント数リンクは、[SQ アラート レポート（SQ Alert Report）] ページを開きます。このページには、クラスタ内の特定のデバイス プールで発生したイベントの詳細が一覧表示されます。

（注）

- デバイス プール名に表示されるのは、そのデバイス プールに対して [電話未登録しきい値超過（Phones Unregistered Threshold Exceeded）] または [サービス品質しきい値超過] アラームが発生したかどうかのフラグです。
- [SQに関する問題（SQ Issues）] カラムのエンドポイントとイベントの数は、過去 4 時間分のみ表示されます。

トポロジ - Cisco Unified Communications Manager または Cisco TelePresence Video Communication Server クラスタ

クラスタ トポロジには、次のクラスタの論理的なトップレベル ビューが表示されます。

- Cisco Unified Communications Manager（Unified CM）
- Cisco TelePresence Video Communication Server（VCS）

クラスタ トポロジ ビューは次の操作に使用できます。

- Unified CM または VCS に登録されているデバイス、それらのデバイスのステータス、およびクラスタ内のデバイスの登録ステータスを確認する。
- アラームを確認し、個々のデバイスやクラスタ レベルでアラームに対処する。
- データベースのレプリケーション ステータスを確認する。
- クラスタ内のデバイスを検索する。

前提条件

- すべてのデバイスが Cisco Prime Collaboration Assurance で管理対象状態になっている必要があります。
- Unified CM パブリッシャが管理対象状態になっている必要があります。
- VCS クラスタが Ops ビュー（現在の名称は [ネットワークの正常性の概要（Network Health Overview）]）に表示されるようにするには、VCS でクラスタ名（VCS の FQDN）を設定する必要があります。

（注）
- トポロジには、パブリック IP アドレスと DNS 名だけが表示されます。

Unified CM または VCS クラスタ トポロジへのアクセス

Cisco Unified CM トポロジ ビューにアクセスするには、次のオプションを選択します。 **[モニタ（Monitor）] > [システム ビュー（System View）] > [OpsView]**。Unified CM クラスタ名をクリックし、[トポロジ（Topology）] タブに移動します。

Cisco VCS のトポロジ ビューにアクセスするには、 **[モニタ（Monitor）] > [システム ビュー（System View）] > [OpsView]**。VCS クラスタをクリックします。

Cisco Prime Collaboration リリース 11.5 以降の場合

Cisco Unified CM トポロジ ビューにアクセスするには、次のオプションを選択します。 **[ネットワーク正常性の概要（Network Health Overview）] > [OpsView]**。Unified CM クラスタ名をクリックし、[トポロジ（Topology）] タブに移動します。

Cisco VCS のトポロジ ビューにアクセスするには、**[ネットワーク正常性の概要（Network Health Overview）]** > **[OpsView]**。VCS クラスタをクリックします。

[トポロジ（Topology）] タブは、Unified CM または VCS のデバイス 360 ビューからも表示できます。デバイス 360 ビューで、クラスタ ID の値をクリックします。そのクラスタの [クラスタビュー（Cluster View）] ページが開きます。ここで [トポロジ（Topology）] をクリックすると、トポロジ ビューが開きます。

クラスタ トポロジ - コンポーネント

Unified CM または VCS クラスタについて、次のコンポーネントまたは詳細が表示されます（該当する場合）。

Unified CM Cluster	**VCS クラスタ**
クラスタ名	クラスタ名
Unified CM	VCS
エンドポイント	エンドポイント
不明なデバイス	Cisco TelePresence Management Suite（TMS）
アプリケーション サーバ	Cisco TelePresence Conductor
ゲートウェイ（H323、MGCP、および SIP）	Cisco TelePresence Server
	Cisco マルチポイント コントロール ユニット
Cisco TelePresence Manager	-
Cisco IM and Presence	-
Cisco TelePresence Conductor	-
Cisco TelePresence Server	-
Cisco マルチポイント コントロール ユニット	-
Cisco Unity Connection	-
Cisco Unified Border Element	-
Cisco TelePresence Multipoint Switch	-
Cisco Unified MeetingPlace	-
Cisco Unified MeetingPlace Express	-
Cisco MediaSense	-
Cisco Unified Customer Voice Portal	-
Cisco Emergency Responder	-

Unified CM Cluster	VCS クラスタ
Cisco Unity Express	-
Cisco Unified Contact Center Express	-
Cisco Unified Contact Center Enterprise	-

Cisco Prime Collaboration リリース 11.5 以降の場合

（注） Unified CM または VCS クラスタでは、Cisco TelePresence Manager、Cisco TelePresence Multipoint Switch、および Cisco Unified MeetingPlace Express は表示されません。

クラスタ間トランク（ICT）の上にマウス ポインタを置くと、ツールチップに次の情報が表示されます。

- ソース
- ゲートキーパーの IP
- ターゲット
- プロトコル
- トランク名

ICT アイコンをクリックすると、ICT クラスタのトポロジ ビューが開きます。Internet Explorer バージョン 11 を使用している場合は、ICT アイコンをクリックするとブラウザが最新の情報に更新されるため、Unified CM トポロジの起動に少し時間がかかります。

（注） ドメインやカスタマーにクラスタを表示する特権がない場合、ICT クラスタのトポロジ ビューは表示されません。

次の間のリンク ステータスが表示されます。

- Unified CM クラスタ：Unified CM と、MGCP、ボイス メール ポート（SCCP を使用する Cisco Unity Connection）、メディア デバイス、CTI ポート、および CTI ルート ポイント
- VCS クラスタ：VCS と、MCU および Cisco TelePresence Server

リンクの上にマウス ポインタを置くと、ツールチップにリンクのステータスが表示されます。

デバイスと Unified CM 間のリンクがダウンしている場合は、リンクをクリックして [登録済みデバイス（Registered Devices）] タブを開くことができます。デバイスの一覧が自動的にフィルタ処理され、[登録ステータス（Registration Status）] が [未登録（Unregistered）] のデバイスが表示されます。他のデバイスの登録ステータスを表示するには、[登録ステータス（Registration Status）] フィールドにフィルタを適用します。

リンクに警告アイコンまたは重大アイコンが表示された場合は、次のような状況を示しています。

- 警告アイコン：登録ステータスまたはリンク ステータスがダウンしています。
- 重大アイコン：登録ステータスとリンク ステータスの両方がダウンしています。

クラスタ内の情報を表示

クラスタから、次の情報を確認できます。

表示オプション

次のいずれかを選択して表示できます。

- デバイスの IP アドレスまたは DNS を選択するか、使用可能なドロップダウンリストから選択して両方のラベルを非表示にします。デフォルトでは、DNS が表示されます。ラベルを非表示にしても、Inter Cluster Trunk や管理されていないおエンドポイントのラベルは非表示になりません。
- すべてのデバイスまたはアラーム付きのデバイス（[アラーム付きのデバイスを表示（Show Devices with Alarms）] チェックボックスを選択）のみが対象です。これはクラウド内のデバイスのみに適用され、Unified CM または VCS ノード、Inter Cluster Trunk（ICT）、[Unmanaged Devices] グループには適用されません。
- 使用可能なドロップダウンから選択することで、[Distributed]、[Hierarchic[、[Circular] レイアウトにマップをクラスタ化します。デフォルトでは、ページには [Circular] レイアウトが表示されます。

以前に使用したブラウザからクラスタ ビューを起動すると、上記の表示オプションが維持されます。

グループに 50 個以上のデバイスがある場合、デフォルトでは、折りたたまれた形式で表示されます。デバイスを表示するには、展開する必要があります。

デフォルトでは、ページは 2 分ごとに更新されます。

クラスタ内のエンドポイント

クラスタの一部とされるすべてのエンドポイントは、1 つのグループとして表示されます。グループ アイコンにポインタを合わせると、ツール ヒントには次の情報が表示されます。

- 合計エンドポイント数
- 登録済みのエンドポイント
- 未登録のエンドポイント（ハードおよびソフト）
- 不明なエンドポイント

エンドポイント グループのクリック ビュー アイコンをクリックし、カウントをクリックすると、選択したエンドポイントで情報がフィルタリングされた[エンドポイントの診断（Endpoint Diagnostics）] ページが起動します。

クラスタ内で管理されていないデバイスの一覧

[Unmanaged] グループ アイコンをクリックすることで、クラスタ内の管理されていないデバイスの一覧を表示できます。[Unmanaged Devices] ポップアップ ウィンドウが表示されます。[Unmanaged Devices] テーブルには、デバイスの IP アドレス/ホスト名、タイプ（デバイス タイプ）、情報へのリンクが表示されます。[Quick Filter] または [Advanced Filter] を使用して、デバイスを検索することができます。

[Unmanaged Devices] ページでは、デバイスを追加または検出できます。およびインベントリ管理からデバイスを検出するには、[デバイスの追加（Add Device）] ボタンをクリックします。

デバイスの詳細

デバイスにカーソルを合わせると、そのデバイスの IP アドレス、ホスト名、ステータス、機能が表示されます。[デバイス 360（Device 360）] ビューを起動するには、デバイス アイコンをクリックします。

Cisco Unified Communications Manager クラスタのデータベース レプリケーション ステータス

緑のタイマー アイコンは、クラスタ内の Cisco Unified Communications Manager 間のデータベース レプリケーションが正常に行われたことを示します。赤色のバツ印は、クラスタ内の Cisco Unified Communications Manager 間のデータベース レプリケーションでエラーがあることを示します。この機能は、Unified CM のみに適用されます。

アラームの詳細

デバイスまたはクラスタでアラームが発生すると、デバイスの横にアラーム アイコンが表示されます。アラームが発生すると、アラームが解消または手動で消去されるまで、トポロジ ビューに表示されたままになります。

デバイスのアラームを表示するには、デバイスをクリックし、[デバイス 360 度（Device 360 degree）] ビューのポップアップ ウィンドウを表示させることで、ウィンドウ下のペインにある [アラーム（Alarm）] タブにアラームが一覧表示されます。

クラスタ レベルのアラームを表示するには、クラスタ クラウドでアラーム アイコンをクリックします。[クラスタ アラーム（Cluster Alarm）] ポップアップ ウィンドウが表示されます。**[アラームの詳細（Alarm Details）]** をクリックし、[アラームとイベント（Alarms & Events）] とクロス起動させます。アラームは、クラスタに基づきフィルタリングされます。

[概要（Summary）] タブに移動することもできます（[OpsView] を選択してクラスタをクリック）。[アラームの概要（Alarm Summary）] ダッシュレットで、クラスタの**[合計（Total）]** 列の値をクリックします。[アラームとイベント（Alarms & Events）] ページが表示されます。アラームは、クラスタに基づきフィルタリングされます。

クラスタ レベルのアラームは、Unified CM クラスタのみに使用できます。

（注） 情報アラームは表示されません。

デバイス アイコンは、次の条件ではグレー表示されます。

- デバイスが、および [インベントリ管理（Inventory Management）] でデバイスが到達不能な状態にある場合。
- デバイスで、*deviceunreachable* アラームが発生する。

[デバイスの検索]

デバイスは、[トポロジ表示（Topology View）]ペインの検索ボックスを使用して、ホスト名やIPアドレス別に検索できます。検索クエリと一致するデバイスは、ボックスとともに強調表示され、中央に移動されます。検索クエリが2台以上のデバイスと一致する場合、これらすべてのデバイスはボックスで強調表示されます。

検索したデバイスが、50台のデバイスを含むグループの一部である場合は、次のようになります。

- グループが以前に展開されていない場合は、グループ全体が強調表示されます。グループの拡張後に強調表示されているデバイスを表示するには、グループを展開する必要があります。
- グループが以前に展開されている場合は、グループはデフォルトで展開され、デバイスが強調表示されます。

（注） 電話機の検索はサポートされていません。

接続済みデバイス

[接続済みデバイス（Connected Devices）] タブは、デバイス タイプ、登録ステータス、IP フィルタに基づき、デバイス検索の実行に役立ちます。

[パフォーマンス（Performance）]

[パフォーマンス（Performance）] タブには、Ops ビューで選択した Unified CM Publisher ノードに基づき、定義済みのダッシュボードが表示されます。**[クラスタまたはデバイス（Cluster or Device）]** ドロップダウン リストから他のクラスタ ノードを選択することはできません。また、カスタム パフォーマンス ダッシュボードを作成することもできます。

作成したカスタム ダッシュボードでは、履歴トレンドを有効にできます。カスタム パフォーマンス ダッシュボードの作成を参照してください。

ルート パターンの概要

ルートパターンの概要には、各ルート グループの使用率とコール音量に関する情報が表示されます。また、クラスタで設定されたルート リストまたはゲートウェイも表示されます。

（注） ルート グループ名のリンクをクリックすると、**[レポート（Report）]** ポップアップ ウィンドウが表示されます。このウィンドウには、選択したルート グループの使用率、コール音量、チャネルの使用状況が表示されます。

次の情報を確認できます。

- ルート リストまたはゲートウェイ
- ルート グループに関連付けられたルート パターン

デバイスの検索

[デバイスの検索（Device Search）] タブでは、選択した Unified CM 内のデバイスを検索できます。詳細については、セクションUnified CM デバイスの検索 （233 ページ）を参照してください。

エンドポイント登録の概要

ネットワークにあるすべてのエンドポイントに関するステータスの概要を示します。E20、電話機、 などのハード エンドポイントや、ソフト クライアント（Cisco Unified Personal Communicator、Cisco IP Communicator、iPhone、Android、Cisco Jabber、Client Services Framework（CSF））、Jabber のエンドポイントなどの概要を個別に表示できます。

前提条件

- すべてのデバイスが Cisco Prime Collaboration Assurance で管理対象状態になっている必要があります。
- クラスタを Cisco Prime Collaboration Assurance で検出する必要があります。

Cisco Prime Collaboration リリース 11.5 以降の場合

前提条件

- クラスタを Cisco Prime Collaboration Assurance で検出する必要があります。

このダッシュボードでは、要約を、円グラフまたはテーブルとして表示します。これは、次のモードのエンドポイントに関する情報を提供します。

- 未登録—Cisco Unified Communications Manager および VCS に登録されていないエンドポイントです。赤で表示されます。[Unregistered from UCM] に表示される数には、Energy Save モードのデバイスが含まれます。

- 登録済み—Cisco Unified CM および Cisco VCS に登録されているエンドポイントです。緑で表示されます。「[Registered Hard Phones]」 で表示される数には、Cisco TelePresence のエンドポイントが含まれています。
- [Unknown]：不明状態（エンドポイントの登録ステータスが不明）のエンドポイント。灰色で表示されます。

Cisco Prime Collaboration リリース 11.1 以前の場合

円グラフをクリックすると、次のページへのリンクを含む [Endpoint Health Troubleshooting] ウィンドウが表示されます。

- エンドポイントの診断
- Phone Report
- UCM Troubleshoot
- VCS Troubleshoot

UC トポロジ ビュー、診断の概要ビュー、エンドポイントの登録概要ダッシュレットに表示される電話機の数は同期されます。同期には最大 10 分の遅延が生じます。必要に応じて、クラスタ検出をスケジュールし、手動で同期をトリガーできます。クラスタ検出では、すべての電話機の登録ステータスも再同期されます。クラスタ検出が手動でスケジュールされていない場合は、夜間のクラスタ検出の一部として同期が実行されます。

可用性の概要

Unified Communications デバイスグループの下に一覧表示されているデバイスの最新データを提供します。

可用性の概要ダッシュレットは、Cisco Prime Collaboration Assurance の各デバイス タイプでサポートされている重大なイベントのサブセットを追跡し、デバイスを **Down** として表示します。イベントの一覧を表示するには、「サービス可用性の概要イベント」を参照してください。イベントの説明とデバイス タイプについては、「Cisco Prime Collaboration Assurance でサポートされているアラームとイベント」を参照してください。

X 軸はアプリケーション数を表示します。Y 軸はアプリケーション タイプを表示します。

緑はアクティブなアプリケーションを示します。赤は、アプリケーションがダウンであることを示します。

バーをクリックしてポップアップを開くと、 ページへのリンクが表示されます。クラスタ ビューと アラーム ブラウザです。

（注） このダッシュレットでは、Cisco Prime Collaboration Assurance にデバイスが追加されていない場合、データは一切表示されません。

サービス エクスペリエンス/コール品質

サービス エクスペリエンス ダッシュボードは、コール品質アラーム、コール品質が不十分な場所、アラームを伴うセッション、コールに失敗した場所など、最も影響を受けている TelePresence エンドポイントの特定に役立ちます。

次のダッシュレットが含まれています。

- Top 5 Poor Voice Call Quality Locations
- Top 5 Call Failure Locations
- Top 10 TelePresence Endpoints with Call Quality Alarms
- アラーム付きの会議

（注） コール品質ダッシュレットには、デバイスの場所がデバイスに割り当てられているデバイス プールの場所と異なる場合、間違った情報が表示されます。デバイスとデバイス プール レベルが同じ場所に設定されていることを確認します。デバイスの場所をシステムの場所のいずれか（Hub_None、Phantom、または Shadow）に設定した場合、[場所（Location）] フィールドには、デバイスで設定されている場所ではなく、デバイス プールで設定されている場所が表示されます。

Cisco Prime Collaboration リリース 11.5 以降の場合

サービス エクスペリエンス ダッシュボードは、コール品質に名前変更されました。

Top 5 Poor Voice Call Quality Locations

直近 1 時間のコール品質が最も乏しかった上位 5 つの場所に関する情報を提供します。直近 1 時間よりも前のコール データは、[Assurance レポート（Assurance Reports）] の下にある [CDR と CMR レポート（CDR & CMR）] レポートから確認できます。

Cisco Prime Collaboration リリース 11.5 以降の場合

直近 1 時間のコール品質が最も乏しかった上位 5 つの場所に関する情報を提供します。直近 1 時間よりも前のコール データは、[レポート（Reports）] の下にある [CDR と CMR レポート（CDR & CMR）] レポートから確認できます。

X 軸はロケーションを示します。Y 軸は低品質コールの数を示します。Z 軸には、低品質コールのパーセンテージがバブルで表示されます。ロケーションで失敗したコールのパーセンテージが 0.5 未満の場合、そのロケーションは無視されます。

Cisco Prime Collaboration Assurance を Enterprise モードで 導入した場合、Top 5 Poor Voice Call Quality レポートには、グローバル選択のドロップダウン（ホームページの右上）で選択した特定のドメインに関連付けられるデータが含まれます。

Cisco Prime Collaboration Assurance を MSP モードで導入した場合、Top 5 Poor Voice Call Quality Locations レポートには、お客様の名前や、特定のお客様に関連付けられているデータ（[ホーム（Home）] > [お客様の概要（Customer Summary）] の順に選択）が含まれます。

（注） このダッシュレットには、Cisco TelePresence コールの詳細は含まれていません。

次の詳細を表示するには、Z 軸のバブルをクリックします。

- クラスタ
- Poor calls
- Total calls

Cisco Prime Collaboration リリース 11.1 以前の場合

[トラブルシュート（Troubleshoot）] をクリックして、[コール品質のトラブルシューティング（Call Quality Troubleshooting）] ページを開きます。[Call Quality Trend] ペインには、ロケーションごとに過去 24 時間の低品質コールが表示されます。[影響を受けたデバイス（Impacted Devices）]ペインには、特定の時間にコールに関与したデバイスが表示されます。[コールの詳細（Call Details）] ペインを開くには、[影響を受けたデバイス（Impacted Devices）] ペインの任意のバーをクリックします。

（注） コールの詳細を表示するには、電話機のアクセス スイッチを監視するか、CDP ネイバー探索を使用して電話機から検出する必要があります。

Top 5 Call Failure Locations

直近 1 時間に最も多くのコール エラーが発生した上位 5 つの場所を表示します。Cisco Prime Collaboration Assurance は、一定の間隔で利用可能な CDR データを集約し、このダッシュレットで表示します。

Cisco Prime Collaboration Assurance に追加される Cisco Unified Communications Manager クラスタを考慮した、上位 5 つの場所が選択されます。たとえば、Cisco Prime Collaboration Assurance で 3 つの Cisco Unified Communications Manager クラスタが追加され、各クラスタには 30 か所の場所がある場合、これら 90 か所のなかから上位 5 つの場所が選択されます。

コールの障害が発生しているロケーションが 5 件未満の場合は、そのロケーションだけが表示されます。ロケーションで失敗したコールのパーセンテージが 0.5 未満の場合、そのロケーションは無視されます。

Cisco Prime Collaboration Assurance を Enterprise モードで 導入した場合、Top 5 Call Failure Locations レポートには、グローバル選択のドロップダウン（ホームページの右上）で選択した特定のドメインに関連付けられるデータが含まれます。

Cisco Prime Collaboration Assurance を MSP モードで導入した場合、Top 5 Call Failure Locations レポートには、お客様の名前や、特定のお客様に関連付けられているデータ（[ホーム（Home）] > [お客様の概要（Customer Summary）] の順に選択）が含まれます。

Z 軸のバブルをクリックすると、次の詳細を表示できます。

- クラスタ
- Failed Calls
- 合計コール数

Cisco Prime Collaboration リリース 11.1 以前の場合

[トラブルシュート（Troubleshoot）]をクリックして、[コール失敗のトラブルシューティング（Call Failure Troubleshooting）] ページを開きます。

Top 10 TelePresence Endpoints with Call Quality Alarms

コール品質アラーム（パケット損失、ジッタ、遅延用）のある上位 10 個のエンドポイントを表示します。

アラーム データをクリックすると、[アラーム（Alarm）] ページが起動します。

アラーム付きの会議

アラームが付いた進行中の会議数を表示します。

このダッシュレットから、**[360 会議ビュー（360 Conference View）]**を起動することができます。

アラーム ダッシュボード

アラーム ダッシュボードは、アラームのある最も影響が大きいテレプレゼンス エンドポイント、アラームのあるデバイス、およびインフラストラクチャ アラームの概要を確認するために役立ちます。

Cisco Prime Collaboration リリース 11.5 以降の場合

アラーム ダッシュボードは、アラームのある最も影響が大きいテレプレゼンス エンドポイント、アラームのあるデバイス、およびデバイス アラームの概要を確認するために役立ちます。

次のダッシュレットが含まれています。

Top 10 TelePresence Endpoints with Alarms

アラームのある上位 10 個の TelePresence エンドポイントを表示します。棒グラフをクリックすると、すべての重大なアラーム カウントの概要が示されたクイック ビューを開くことができます。アラーム カウントには重大度 Cleared のアラームが含まれます。

アラーム数の合計をクリックすると、Alarm ブラウザでクロス起動させ、アラームの詳細を表示できます。エンドポイントおよびサービス インフラストラクチャ デバイスのグラフを表示できます。

Top 10 Devices with Alarms

アラームのある上位 10 台のデバイスを表示します。棒グラフをクリックすると、すべての重大なアラーム カウントの概要が示されたクイック ビューを開くことができます。アラーム カウントには、重大度がクリアされたアラームが含まれます。

アラーム数の合計をクリックすると、Alarm ブラウザでクロス起動させ、アラームの詳細を表示できます。エンドポイントおよびサービス インフラストラクチャ デバイスのグラフを表示できます。

およびインベントリ管理を起動し、エンドポイントまたはサービスインフラストラクチャのいずれかのリンクをクリックして、デバイスの詳細を表示できます。

（注） クラスタは、デバイスとして扱われないため、このダッシュレットに表示されません。

インフラストラクチャ アラームの概要/デバイス アラームの概要

アラームの有無にかかわらずインフラストラクチャデバイスの数を表示します。また、アラームの重大度に基づいて、デバイスの数を表示することもできます。

合計デバイス データをクリックして、[デバイス インベントリ（Device Inventory）] ページを起動できます。[Alarms and Events] ページを表示するには、アラームのデータ デバイスもクリックできます。

デフォルトでは、情報は円グラフで表示されます。ユーザインターフェイスが更新されると、円グラフが更新されます。この表示は表に変更できます。

Cisco Prime Collaboration リリース 11.5 以降の場合

（注） [インフラストラクチャ アラームの概要（Infrastructure Alarm Summary）] ダッシュレットの名前が [デバイス アラームの概要（Device Alarm Summary）] に変更されます。

使用率モニタ

[使用率の監視（Utilization Monitor）]**[監視（Monitor）] > [使用率の監視（Utilization Monitor）]** 使用率モニタ（[操作（Operate）] > [使用率の監視（Utilization Monitor）] または [モニタ（Monitor）][使用率の監視（Utilization Monitor）] の順に移動）ページには、トランクの使用率、トランク/ルート グループの使用率、ロケーションによる CAC バンド幅の使用率、会議デバイス、および コンダクタ ブリッジ プールの使用率、

（注） Cisco Prime Collaboration Assurance は、ゲートウェイの管理で SNMPv2c および SNMPv3 をサポートしています。ただし、Cisco Prime Collaboration Assurance では、SNMPv3 を使用したパフォーマン スポーリング（GSU）はサポートされていません。

トランク使用率

Cisco Prime Collaboration リリース 11.1 以前の場合

チャネル使用に関して、使用率が最も高いトランクに関する情報を提供します。

使用率、関連付けられているゲートウェイ IP と名前、関連付けられたルート グループの詳細を確認できます。

CCisco Prime Collaboration Assurance では、SIP トランクの最大キャパシティを設定できます。[SIP トランクのキャパシティ設定（SIP Trunks Capacity Settings）] リンクをクリックし、[SIP トランクの最大キャパシティ（SIP Trunk Max Capacity）] タブで Border Element のゲートウェイを選択し、Border Element の IP を選択します。SIP トランクを通過できる最大コール数を指定します。

（注） [SIP トランクのキャパシティ設定（SIP Trunks Capacity Settings）] リンクにアクセスするには、管理者権限が必要です。

[使用率（Utilization）] 列のパーセンテージ リンクをクリックすると、時間に対してプロットされたトランクの使用率がグラフで表示されます。最後のポーリング サイクルのデータが表示されています。

4 分間の各インターバルに対する X 軸座標にカーソルを配置すると、パーセンテージとして使用率を表示するポップアップを表示できます。トランクまたはルートの使用率を表示する詳細なパフォーマンス グラフを開くには、グラフのポイントをクリックするか、X 軸座標に対応するチャネル使用率バーをクリックします。

（注） Cisco Prime Collaboration Assurance では、HSRP 対応デバイスはサポートされていません。

次の表には、Cisco Prime Collaboration Assurance にある、さまざまなタイプの SIP トランクの使用率レポートに関する概要が示されています。

表 *58 : SIP* トランク タイプの使用率レポート

SIP トランクのタイプ	使用率レポート	
	データ ソース	サポート
クラスタ間トランク	CDR	提供されています。これらトランクは、クラスタ間トランクが Unified Communications Manager の場合はデータを表示させず、データを正しく表示する必要がある場合は、これらのトランクをボイス ゲートウェイに関連付けさせます。

SIP トランクのタイプ	使用率レポート	
Cisco Unified Border Element（CUBE）に接続した SIP トランク	CUBE を直接ポーリング	Available
UCM SIP トランク（これらのトランクはサービス プロバイダーによって提供されるのではなく Enterprise 管理者が作成します）たとえば、ICT や Trunk to Webex などです。	RTMT UCM SIP パフォーマンス カウンタ	該当なし。RTMT パフォーマンス ダッシュボードのみで、指定時間のコール ボリュームを確認することができます。
CUBE に接続していない SIP トランク（たとえば、ACME）です。	RTMT UCM SIP パフォーマンス カウンタ	該当なし。RTMT パフォーマンス ダッシュボードのみで、指定時間のコール ボリュームを確認することができます。

（注） Cisco Integrated Services Routers（ISR）および Cisco ISR G2 は必要な SNMP ツールを提供するプラットフォームではないため、T1/E1 Channel Associated Signaling（CAS）トランクの使用率を監視することはできません。

Cisco Prime Collaboration リリース 11.5 以前の場合

（注） Cisco Prime Collaboration Assurance は、Cisco Unified Border Element（CUBE）に接続している SIP トランクの使用率のみをサポートします。Cisco Prime Collaboration Assurance は、Unified Communications Manager で設定された SIP トランクの使用率はサポートしません。

T1/E1 トランク

Cisco Prime Collaboration リリース 11.5 以降の場合

チャネル使用に関して、使用率が最も高い T1/E1 トランクに関する情報を提供します。

使用率、関連付けられているゲートウェイ IP と名前、関連付けられたルート グループの詳細を確認できます。

[使用率（Utilization）] 列のパーセンテージ リンクをクリックすると、時間に対してプロットされたトランクの使用率がグラフで表示されます。最後のポーリング サイクルのデータが表示されています。

4 分間の各インターバルに対する X 軸座標にカーソルを配置すると、パーセンテージとして使用率を表示するポップアップを表示できます。トランクまたはルートの使用率を表示する詳細なパフォーマンス グラフを開くには、グラフのポイントをクリックするか、X 軸座標に対応するチャネル使用率バーをクリックします。

（注） Cisco Prime Collaboration Assurance では、HSRP 対応デバイスはサポートされていません。

（注） Cisco Integrated Services Routers（ISR）および Cisco ISR G2 は必要な SNMP ツールを提供するプラットフォームではないため、T1/E1 Channel Associated Signaling（CAS）トランクの使用率を監視することはできません。

CUBE SIP トランク

Cisco Prime Collaboration リリース 11.5 以降の場合

チャネル使用に関して、使用率が最も高い SIP トランクに関する情報を提供します。

SIP トランクの使用率、最大同時コールのデフォルト値、Cisco Unified Border Element （CUBE）で設定されている最大同時コールの値、ならびに関連付けられている CUBE IP の詳細が表示されます。

（注） [最大同時コール数（キューブで設定）] 列には、CUBE のダイヤル ピア レベルで設定した最大コール数が含まれます。

Cisco Prime Collaboration Assurance では、CUBE が接続した SIP トランクの最大同時コール数を設定できます。[SIP トランク（SIP Trunk）] ページで、設定する SIP トランクに対応するチェックボックスをオンにします。**[最大同時コール数の設定（Set Max Concurrent Call）** ボタンをクリックし、Cisco Prime Collaboration Assurance の SIP トランクを通過できる最大同時コール数を指定します。

[使用率（Utilization）] 列のパーセンテージ リンクをクリックすると、時間に対してプロットされた SIP トランクの使用率がグラフで表示されます。最後のポーリング サイクルのデータが表示されています。

4 分間の各インターバルに対する X 軸座標にカーソルを配置すると、パーセンテージとして使用率を表示するポップアップを表示できます。トランクまたはルートの使用率を表示する詳細なパフォーマンス グラフを開くには、グラフのポイントをクリックするか、X 軸座標に対応するチャネル使用率バーをクリックします。

Cisco Prime Collaboration リリース 12.1 以降の場合

Cisco Prime Collaboration Assurance ユーザ インタフェイスで、**[使用率モニタ（Utilization Monitor）]** ページから**[監視（Monitor）]** > **[使用率モニタ（Utilization Monitor）]** > **[CUBE SIP トランク（CUBE SIP Trunk）]** タブへと移動すると、セッション サーバ グループ 設定の CUBE SIP トランクを表示できます。

[CUBE SIP トランク（CUBE SIP Trunk）] ページで、サーバ グループ設定に対応するチェックボックスをオンにし、[Raise/Suppress] ボタンを有効にします。デフォルトでは、アラームは **[Raise]** 状態になっています。この状態は、変更した場合のみ更新されます。

[Alarm Status] 列は、アラームを高めることができるどうかを示します。

次の表には、Cisco Prime Collaboration Assurance にある、さまざまなタイプの SIP トランクの使用率レポートに関する概要が示されています。

表 *59 : SIP* トランク タイプの使用率レポート

SIP トランクのタイプ	使用率レポート	
	データ ソース	サポート
クラスタ間トランク	CDR	提供されています。これらトランクは、クラスタ間トランクが Unified Communications Manager の場合はデータを表示させず、データを正しく表示する必要がある場合は、これらのトランクをボイス ゲートウェイに関連付けさせます。
Cisco Unified Border Element（CUBE）に接続した SIP トランク	CUBE を直接ポーリング	Available
UCM SIP トランク（これらのトランクはサービス プロバイダーによって提供されるのではなく Enterprise 管理者が作成します）たとえば、ICT や Trunk to Webex などです。	RTMT UCM SIP パフォーマンス カウンタ	該当なし。RTMT パフォーマンス ダッシュボードのみで、指定時間のコール ボリュームを確認することができます。
CUBE に接続していない SIP トランク（たとえば、ACME）です。	RTMT UCM SIP パフォーマンス カウンタ	該当なし。RTMT パフォーマンス ダッシュボードのみで、指定時間のコール ボリュームを確認することができます。

（注） Cisco Prime Collaboration Assurance は、Cisco Unified Border Element（CUBE）に接続している SIP トランクの使用率のみをサポートします。Cisco Prime Collaboration Assurance は、[UCM SIP Trunk] ページで Unified Communications Manager に設定されている SIP トランクの使用率をサポートします。

Cisco Prime Collaboration リリース 11.6 以降の場合

Cisco Prime Collaboration Assurance は、CUBE が接続した SIP トランクと、Unified Communications Manager で設定した SIP トランクの両方の使用率をサポートします。

SIP トランクの最大同時コール数のデフォルト値を変更

スーパー管理者、システム管理者、ネットワーク オペレータは、キューブが接続した SIP トランクの最大同時コール数のデフォルト値を設定することができます。

前提条件：このタスクを実行するには root アクセス機能が必要です。そのため、root アクセス権を取得するために TAC ケースを送信する必要があります。

SIP トランクの最大同時コール数のデフォルト値を設定するには、次の手順に従います。

1. root ユーザとしてログインします。
2. `/opt/emms/cuom/gpf` フォルダに移動して、*gpf.properties* ファイルを編集します。
3. および **SipTrunkMaxCapacity=100** 列を見つけて、値を「100」から目的の数値に変更します。
4. 管理者ユーザでログインして Cisco Prime Collaboration Assurance サーバを再起動させ、次のコマンドを実行します。
    1. **<hostname>/admin#application stop cpcm**
    2. **<hostname>/admin#application start cpcm**

UCM SIP トランク

Cisco Prime Collaboration リリース 11.6 以降の場合

Unified Communications Manager クラスタに接続しているすべての SIP トランクに関する情報を提供します。

[UCM SIP トランク（UCM SIP Trunk）] が、タブとして [使用率の監視（Utilization Monitor）] ページに追加されました。**[監視（Monitor）]** > **[使用率の監視（Utilization Monitor）]** > **[UCM SIP トランク（CUBE SIP Trunk）]** の [Cisco Prime Collaboration Assurance ユーザ インターフェイス（Cisco Prime Collaboration Assurance User Interface）]

SIP トランクの使用率（音声およびビデオの最大コール数やアクティブ コールの合計数）、最大同時コール酢のデフォルト値、SIP トランクのステータス、フラグが表示されます。

（注） [使用率（Utilization）]列には、音声コールとビデオコールの両方の使用率に関する詳細が含まれます。

ステータス	説明
シングル	SIP トランクがクラスタ内の 1 つのノード上で実行されています。
マルチ	SIP トランクがクラスタ内の複数のノード上で実行されています。
すべてのノード上で実行	SIP トランクがクラスタ内の全てのノード上で実行されています。

（注） [Single] または [Multiple] ステータスの SIP トランクでは、特定の SIP トランクを [SIP トランク名（SIP Trunk Name）] 列から展開すると、リモート先に関する情報や、各ノードの音声およびビデオのコール ステータスなどの情報を含む、その他のテーブルを表示することができます。

Cisco Prime Collaboration Assurance では、複数の SIP トランクの音声またはビデオで最大同時コール数を設定できます。[SIP トランク（SIP Trunk）] ページで、設定する SIP トランクに対応するチェックボックスをオンにします。**[最大同時コール数（Max Concurrent Call）** ボタンをクリックし、Cisco Prime Collaboration Assurance の SIP トランクを通過できる最大同時コール数を指定します。[Audio Max Calls] および [Video Max Calls] 列は、入力した値で設定されます。[最大同時コール数（Max Concurrent Call）] オプションを使用して音声およびビデオの最大コール数値を設定しなかった場合、Unified Communications Manager のデフォルト値を使用して 2 つの列が追加されます。

（注）
- [OpsView] タブでは、[UCM SIP トランク（UCM SIP Trunks）] ページにクロス起動することもできます。
- UCM SIP トランクは、MSP モードではサポートされていません。

ルート グループの使用率

チャネル使用について、最も利用されるルート グループの情報を提供します。

また、使用率や関連するクラスタの詳細を表示することもできます。[使用率（Utilization）]列のパーセンテージ リンクをクリックすると、時間に対してプロットされたルート グループの使用率がグラフで表示されます。最後のポーリング サイクルのデータが表示されています。

ルート グループを選択すると、[関連付けられているゲートウェイ/トランク（Associated Gateways/Trunks）] テーブルを表示できます。この表には、トランク、ゲートウェイ名、ゲートウェイ IP に関する情報が含まれています。[保存（Save）] をクリックして、選択したトランクをルート グループに追加します。

（注） トランクがルート グループに関連付けられている場合でも、ポーリングが実行されないと、[データがありません（No Data Available）] エラーが表示されます。

（注） [使用率（Utilization）] 列には、ルート グループに対してトランクを選択しなかった場合、「[トランクが選択されていません（Trunks Not Selected）]」 メッセージが表示されます。

4 分間の各インターバルに対する X 軸座標にカーソルを配置すると、パーセンテージとして使用率を表示するポップアップを表示できます。トランクまたはルートの使用率を表示する詳細なパフォーマンス グラフを開くには、グラフのポイントをクリックするか、X 軸座標に対応するチャネル使用率バーをクリックします。

Cisco Prime Collaboration リリース 11.1 以前の場合

Cisco Prime Collaboration Assurance では、ルート グループの集計を計算することができます。[ルート グループの集計設定（Route Group Aggregation Settings）] リンクをクリックし、[トランクの使用設定 （Trunk Utilization Settings）] ページで [ルート グループ集計（Route Group Aggregation）] タブをクリックします。Unified Communication System（UCS）クラスタ、ルートグループの順に選択し、指定したルート グループに属するトランクを選択します。

（注） [ルート グループの集計設定（Route Group Aggregation Settings）] リンクにアクセスするには、管理者権限が必要です。

Cisco Unified Border Element（CUBE）に POTS ダイヤル ピアや T1/E1 音声インターフェイスが設定されている場合でも、[トランクの使用設定 （Trunk Utilization Settings）] の下にある [ゲートウェイ（Gatewa）] フィールドには値が表示されず、CUBE として識別されるには、*/opt/emms/emsam/conf/cube_ip.txt* ファイルに IOS IP アドレスを入力します。

トラブルシューティング

問題 : 正しいルート グループが表示されません。

推奨事項 : ルート グループが Unified Communication Manager のルート リストに関連付けられていることを確認し、再検出します。

トランク グループの使用率

チャネル使用に関して、使用率が最も高いトランク グループに関する情報を提供します。

（注） トランクグループのポーリングが行われない場合、[使用可能なデータがありません（No Data Available）] というエラー メッセージが表示されます。

ユーザ定義のトランク グループを作成できます。[トランク グループ設定（Trunk Group Settings）] リンクをクリックし、[トランク使用率の設定（Trunk Utilization Settings）] ページで、[カスタムトランク グループの管理（Custom Trunk Group Management）] タブをクリックします。トランクを選択し、[新規グループの追加（Add New Group）] ボタンをクリックします。[新規グループ（New Group）] ダイアログ ボックスが表示されます。詳細を入力し、[保存（Save）] をクリックします。グループが正常に作成されたことを知らせるメッセージが表示されます。ユーザが定義した既存のトランク グループに他のデバイスを追加するには、[グループに追加（Add to Group）] ボタンをクリックします。ユーザが定義したすべてのグループは、ユーザ インターフェイスの左側にある [カスタム トランク グループ（Custom Trunk Group）] ペインに一覧表示されます。[カスタムトランク グループ（Custom Trunk Group）] の下にある検索フィールドを使用して、ユーザ定義のトランクグループを検索することができます。ユーザが定義したこれらのトランクグループが、使用率の高い上位 10 個のトランク グループである場合、それらの使用情報は、[トランク（Trunk）] の下にあるダッシュレットに表示されます。

（注） [トランク グループ設定（Trunk Group Settings）] リンクにアクセスするには、管理者権限が必要です。

[使用率（Utilization）] 列のパーセンテージ リンクをクリックすると、時間に対してプロットされたトランクの使用率がグラフで表示されます。最後のポーリング サイクルのデータが表示されています。

4 分間の各インターバルに対する X 軸座標にカーソルを配置すると、パーセンテージとして使用率を表示するポップアップを表示できます。トランクまたはルートの使用率を表示する詳細なパフォーマンス グラフを開くには、グラフのポイントをクリックするか、X 軸座標に対応するチャネル使用率バーをクリックします。

Cisco Prime Collaboration リリース 11.6 以降の場合

（注） [ルート グループの使用率（Route Group Utilization）] ページと [トランク グループの使用率（Trunk Group Utilization）] ページの両方では Unified Communications Manager SIP トランクも一覧表示され、ルート グループとトランク グループの両方の使用率を計算します。

Location CAC 帯域幅の使用状況

帯域幅の使用率が最も高くなるの場所についての情報を提供します。

場所の名前、関連付けられているクラスタ、最大帯域幅、使用率、および失敗したコールの数の詳細を表示できます。

[コール失敗（Calls Failed）] 列の [失敗したコール（Failed Calls）] アイコンをクリックして、[リソース不足の場所（Location Out of Resource）] パフォーマンス グラフを起動してください。

デフォルトでは、失敗したコールの数に基づいてテーブルがソートされます。

最大帯域幅の値が [無制限（Unlimited）] または [なし（None）] に設定されている場合、ポーリングは行われず、テーブルにデータは表示されません。

データは 4 分ごとにポーリングされます。

Cisco Prime Collaboration Assurance でのロケーションのポーリングは、ロケーション帯域幅マネージャ サービスが有効になっている Unified CM ノードから実行されます。ロケーション帯域幅マネージャは、任意の Unified CM サブスクライバ上で実行されるか、またはクラスタ内の専用 Unified CM サーバ上で、スタンドアロン サービスとして実行されます。クラスタ内の拡張ロケーション CAC を有効にするには、各クラスタで少なくとも 1 つのロケーション帯域幅マネージャのインスタンスが実行されている必要があります。

（注） Cisco Unified Communications Manager で、**Use Video Bandwidth for Immersive** パラメータを True に設定すると、Cisco Prime Collaboration Assurance はイマーシブ カウンタをポーリングしないため、イマーシブ帯域幅のテーブルにデータが表示されません。

会議デバイス

ネットワーク内の会議デバイスを表示します。

次の詳細情報を表示できます。

- [Status]：デバイスが正常であるか、一時停止されているか、またはエラーを含んでいるかを表示します。ステータス アイコンをクリックして、[Alarm ブラウザ] を起動できます。

  このアイコンは、重要なサービス インフラストラクチャ、到達不能、またはアクセス不能なアラームがある場合に表示されます。

- [Name] および [IP Address]：ブラウザで起動するには、デバイス名または IP アドレスをクリックできます。

  次の情報を表示するには、[Name] 列の上にマウス ポインタを置き、クイック ビュー アイコンをクリックします。

  - メディア処理エンジン、コール制御プロセス、会議マネージャ、セキュリティ キー交換。
  - オーディオ ロード、ビデオ ロード、メディア ロード、使用中のビデオ ポート、バッテリ ステータス、温度ステータス、および電圧ステータス（MCU に関してのみ）
  - CPU およびメモリの使用率。

- デバイス タイプ
- 使用したビデオ ポート

- 使用した音声ポート
- Master Conductor

Click the utilization value of [ビデオポート（Video Ports）] または [使用されているオーディオポート（Audio Ports Used）] 列の使用状況お値をクリックすると、[ビデオポートの使用状況の詳細（Detailed Video Port Utilization）] または [オーディオポートの使用状況の詳細（Detailed Audio Port Utilization）] グラフが開きます。表示するデータとして、パーセント単位の使用率、使用率の絶対値、または両方（[すべて（All）] をクリック）を選択できます。また、スライダを使用して短い時間間隔（1 分間など）を選択して、その時間内の実際のデータを確認することもできます。この情報を使用すると、使用状況に応じてポートの数を増やすことができます。

使用状況は、デバイスが Cisco Prime Collaboration Assurance で初めて管理対象状態になった時点から表示されます。たとえば、デフォルトではグラフに 5 日間のデータを表示できますが、デバイスが 4 日間しか管理対象状態になっていない場合は、4 日間のデータが表示されます。

Conductor Bridge Pool の使用率

ネットワーク内のコンダクタ プールごとに、会議ブリッジの累積使用状況に関する情報を提供します。

次の詳細情報を表示できます。

- [ステータス（Status）] : 各コンダクタ プールに関連付けられている会議ブリッジのステータスに基づいて、コンダクタ プールのステータスを表示します。ステータス アイコンをクリックすると、アラーム ブラウザをクロス起動して、コンダクタ プール内の会議ブリッジの個々のステータスを確認できます。
- [プール名（Pool name）] : プール名をクリックすると、デバイス ウィンドウを個別のブラウザでクロス起動できます。
- [使用されているビデオポート（Video Ports Used）] : [ビデオポート/スクリーンライセンスの使用状況（Video Ports/Screen License Utilization）] 列の使用状況の値をクリックすると、[ビデオポートコンダクタの使用状況の詳細（Detailed Video Port Conductor Utilization）] グラフが開きます。使用状況は、パーセンテージまたは絶対値で表示するように選択できます。また、スライダを使用して短い時間間隔（1 分間など）を選択して、その時間内の実際のデータを確認することもできます。この情報を使用すると、使用状況に応じてポートの数を増やすことができます。使用状況は、デバイスが Cisco Prime Collaboration Assurance で初めて管理対象状態になった時点から表示されます。たとえば、グラフではデフォルトで 7 日間のデータを表示できます。

（注） Cisco Prime Collaboration Assurance では、Cisco TelePresence Conductor のスクリーン ライセンス モードだけがサポートされます。

- Conference Bridge Type

- Conductor Name

（注） 使用状況モニタを表示するには、コンダクタ プールに少なくとも 1 つの会議ブリッジが存在している必要があります。

TelePresence エンドポイント

このダッシュボードを使用して、No Show エンドポイント、最も一般的に使用された、および使用頻度の低い TelePresence エンドポイントとエンドポイント モデルを識別できます。

（注） IP 電話とソフトウェア クライアントの詳細は、TelePresence 使用率レポートには含まれません。

Cisco Prime Collaboration リリース 12.1 SP2 以降の場合

Telepresence エンドポイントの前提条件

Telepresence エンドポイントには、次のものが必要です。

- Unified CM および Cisco VCS は、Managed 状態にある必要があります。
- MCU などのエンドポイントとコントローラは、Managed 状態にある必要があります。
- デバイスの可視性を 「Full Visibility」 状態に設定します。
- JTAPI が Unified Communications Manager で設定されている必要があります。Unified Communications Manager で JTAPI を有効にする方法については、「Cisco Prime Collaboration Assurance のデバイス設定」を参照してください。
- Cisco Prime Collaboration Assurance サーバが、Cisco VCS でフィードバック サーバとして登録されている必要があります。
- 会議の診断と音声電話機能の模擬テストを正しく実行するには、Cisco Prime Collaboration Assurance Service Pack 1 バンドルを適用する前に、CUCM がリストされているバージョンであることを確認してください。詳細については、12.1 Service Pack 1 の『Cisco Prime Collaboration Assurance でサポートされているデバイス』を参照してください。

次のダッシュレットが含まれています。

Top 10 Utilized TelePresence Endpoints

ネットワークの使用率が高い上位 10 個のエンドポイントを表示します。

グラフは、期間、または会議別に表示できます。

- 時間別—使用時間ごとの使用率です。たとえば、使用率が 0.634 時間と表示されている場合、エンドポイントはおよそ 38 分間使用されていたことになります（0.634 x 60）。

- 会議別：使用率が会議の数で示されています。ここでは、完了した会議のみが対象です。会議の数が 1 の場合、x 軸の値は 10 進数で表示されます（0.2、0.4 など）。会議の数が 2 以上の場合、x 軸の値は絶対数（1、2、3 など）で表示されます。

棒グラフをクリックすると、選択したエンドポイントの All Conference Summary レポートを開くことができます。

Top 10 Utilized TelePresence Endpoint Models

特定のエンドポイント モデルに基づいて使用率を表示します。

次のデータを表示できます。

- [For a day]：最大使用率は 10 時間です。したがって、1 日の使用時間が 120 分であれば、1 日の使用率は 20%（（120/（10*60））*100）となります。
- [For a week]：最大使用率は 50 時間です。したがって、1 週間の使用時間が 1500 分であれば、1 週間の使用率は 50%（（1500/（50*60））*100）となります。
- [For four weeks]：最大使用率は 200 時間です。したがって、1 か月の使用時間が 10800 分であれば、1 か月の使用率は 90%（（10800/（200*60））*100）となります。

棒グラフをクリックして、選択されたエンドポイント モデルの [Endpoint Utilization Report] を起動できます。

Top 10 No Show TelePresence Endpoints

スケジュール設定された会議に参加しなかった、上位 10 個のエンドポイントを表示します。

棒グラフをクリックすると、選択したエンドポイントの No Show Conference Summary レポートを開くことができます。

Least 10 Utilized TelePresence Endpoints

ネットワークの使用率が低い下位 10 個のエンドポイントを表示します。

グラフは、期間、または会議別に表示できます。

- 時間別—使用時間ごとの使用率です。たとえば、使用率が 0.634 時間と表示されている場合、エンドポイントはおよそ 38 分間使用されていたことになります（0.634 * 60）。

  使用率がゼロの場合、棒グラフには表示されません。このデータを表示するには、表形式を起動する必要があります。

- 会議別：使用率が会議の数で示されています。ここでは、完了した会議のみが対象です。会議の数が 1 の場合、x 軸の値は 10 進数で表示されます（0.2、0.4 など）。会議の数が 2 以上の場合、x 軸の値は絶対数（1、2、3 など）で表示されます。

棒グラフをクリックすると、選択したエンドポイントの All Conference Summary レポートを開くことができます。

Least 10 Utilized TelePresence Endpoint Models

特定のエンドポイントモデルに基づいて使用率を表示します。使用率がゼロの場合、棒グラフには表示されません。このデータを表示するには、表形式を起動する必要があります。

次のデータを表示できます。

- [For a day]：最大使用率は 10 時間です。したがって、1 日の使用時間が 120 分であれば、1 日の使用率は 20%（（120/（10*60））*100）となります。
- [For a week]：最大使用率は 50 時間です。したがって、1 週間の使用時間が 1500 分であれば、1 週間の使用率は 50%（（1500/（50*60））*100）となります。
- [For four weeks]：最大使用率は 200 時間です。したがって、1 か月の使用時間が 10800 分であれば、1 か月の使用率は 90%（（10800/（200*60））*100）となります。

棒グラフをクリックして、選択されたエンドポイント モデルの [Endpoint Utilization Report] を起動できます。

TelePresence 会議の数

進行中と完了した会議の数を表示します。チャートをクリックして、特定の会議で得られた、Conference Detail レポートを起動します。

会議データは、2 時間ごとに集計されます。たとえば、1 日に 2 回の会議のみが開かれたとします。最初の会議は 01:00 に開始して 03:00 に終了し、2 回目の会議は 02:20 に開始して 05:50 に終了したとします。

データは次のように表示されます。

- 0:00—Zero
- 2:00—1：01:00 から 03:00 まで会議が進行中というデータが、0:00 から 02:00 の間に表示されます。
- 4:00—2：01:00 から 03:00 の間に会議が完了、ならびに 02:20 から 05:50 まで会議が進行中というデータが、02:00 から 04:00 の間に表示されます。
- 6:00—1：02:20 から 05:50 の間に会議が完了というデータが、04:00 から 06:00 の間に表示されます。
- 8:00—Zero：06:00 から08:00 の間に会議は行われませんでした。
- 10:00—Zero
- 12:00—Zero
- ...
- 24:00—Zero：22:00 から 24:00 の間に会議は行われませんでした。

データは、チャートまたは表形式で表示されます。Excel シートにデータをエクスポートすることもできます。

ライセンスの使用状況（License Usage）

[ライセンスの使用状況（License Usage）] タブには、Prime License Manager（すべての UC アプリケーション ライセンスの使用状況）、VCS（VCS クラスタ ライセンスの使用状況）、Contact Center Enterprise ライセンス（CCE ライセンスの使用状況）に関するライセンス情報が表示されます。次のポートレットが含まれています。

- Prime License Manager
- VCS ライセンスの使用状況
- Customer Voice Portal ライセンスの使用率 （394 ページ）
- Contact Center Enterprise ライセンスの使用状況 （395 ページ）

Prime License Manager

音声のライセンス情報は、Prime License Manager ライセンスの下に分類されています。このダッシュレットには、すべての Unified Communications アプリケーション ライセンス（Cisco Unified CM および Cisco Unity Connection）の使用状況が表示されます。ELM と Unified CMが共存する場合は、Enterprise License Management Resource API を手動でアクティブにする必要があります。リストについては、「Cisco Prime Collaboration Assurance のデバイスのセットアップ」と「Cisco Prime Collaboration Assurance のデバイス設定」を参照してください。

次の詳細情報を表示できます。

- [ライセンスのタイプ（License Type）]：CUWLPremium、CUWLStandard、UCM Advanced など、利用可能なさまざまなライセンスのタイプが表示されます。
- [製品の：ライセンスのタイプが属する製品タイプ。
- [ステータス（status）]：ライセンスのタイプのステータス。有効、違反、またはデモが表示されます。
- [残り（Remaining）]：各ライセンスのタイプの使用可能なライセンス数または未使用のライセンス数。

このダッシュレットは、毎晩の CDT 検出が完了した後に、デフォルトで 1 回設定されます。このダッシュレットは、CDT 検出 のたびに更新されます。

トラブルシューティング

問題：Cisco Prime Collaboration Assurance 11.6 では、Standalone Prime Licensing Manager（PLM）が非 Cisco デバイスとして表示されます。

推奨アクション：これは、PLM で SNMP コミュニティ文字列が設定されているときに発生する可能性があります。PLM を適切に検出するには、コミュニティ文字列が設定されていないことを確認します。設定されている場合は削除し、Cisco Prime Collaboration Assurance で PLM 検出を続けます。基本的に、PCA は、PLM ディスカバリ用の SNMP コミュニティ文字列設定をサポートしていません。

（注） 共存している PLM がすべて OS 管理者ユーザを使用してライセンス情報を取得するわけではありません。CUCM で作成されたユーザ ロールによって異なります。ほとんどの顧客導入環境では、Web 管理者は CLI/OS 管理者に権限を割り当てられています。Cisco Prime Collaboration Assurance では、このユーザからライセンス情報を取得できます。

VCS ライセンスの使用状況

すべての VCS クラスタ、クラスタ内の各 VCS サーバ、スタンドアロン VCS サーバ、Cisco Expressway-Core、Cisco Collaboration Edge または Core 搭載の Cisco Expressway-Edge または VCS ライセンスの使用状況が表示されます。Cisco Expressway-Core および Cisco Expressway-Edge クラスタの場合、前回の再起動以降の最大コール数は **[Expressway Peak Concurrent Video Calls]** 列に表示されます。

（注） 最大コール数を表示するには、ライセンスをインストールする必要があります。VCS クラスタでは、ライセンスがインストールされていないまたは値が 0 の場合、最大コール数の列には [N/A] と表示されます。

このダッシュレットは自動更新されません。現在のデータを取得するには、ダッシュレットを更新する必要があります。

VCS バージョン 7.0 以降では、クラスタ ピアにインストール済みのトラバーサルまたは非トラバーサル コールライセンスは、クラスタ内の任意のピアで使用できます。バージョン 7.0 以前では、ライセンスはクラスタ間で共有されません。各ピアは、そのピアにインストール済みのライセンスのみを使用できます。

1 つのピアにインストールできるライセンス数は、次のように、各 VCS ユニットの最大容量に制限されています。

- 500 回の非トラバーサル コール
- 100 回のトラバーサル コール
- 2,500 台の登録

登録ライセンスは、クラスタ間では共有されません。クラスタ ピアが使用できなくなった場合は、そのピアにインストールされた共有可能なライセンスは、ピアへの接続をクラスタが失った時から 2 週間の期間中、残りのクラスタ ピアにそのまま使用できます。これにより、クラスタの全体的なライセンス キャパシティが維持されます。ただし、上記のとおり、各ピアはその物理キャパシティによって引き続き制限されます。この 2 週間の期間が過ぎると、使用できないピアに関連付けられたライセンスがクラスタから削除されます。クラスタの容量を同じに維持するには、ピアの問題を解決するか、新しいオプション キーをクラスタ内の別のピアにインストールするかのいずれかを実行する必要があります。

Customer Voice Portal ライセンスの使用率

Customer Voice Portal（CVP）ライセンスの使用率は、Prime License Manager ライセンスの下に分類されます。このダッシュレットに CVP コール サーバのライセンスの使用率が表示されます。

前提条件：

- コール サーバ機能を備えた CVP は、インベントリ管理で管理対象状態になっている必要があります。
- Contact Center Assurance License が使用できる必要がある。

このダッシュレットには、ポーリング データの時間間隔に基づいてエントリが表示されます。デフォルトのポーリング間隔は 4 分です。

このダッシュレットには、過去 7 日間のポーリング レコードの最新カウントが表示されます。

次の詳細情報を表示できます。

- デバイス：CVP コール サーバ
- [使用中のポート（Ports In Use）]：使用されているポートの数
- [利用可能なポート（Ports Available）]：利用可能なポートの数
- [要求されたポート（Ports Requested）]：要求されたポート数
- [拒否されたポート要求（Ports Requests Denied）]：拒否されたポート要求の数

Contact Center Assurance License の有効期限が切れた場合、CVP ライセンスのダッシュレットには、CVP コール サーバのライセンス使用状況が表示されません。この機能を継続して使用するには、必要な数の Cisco Prime Collaboration Contact Center Assurance の同時使用エージェント ライセンスを購入する必要があります。ライセンスの詳細については、「ライセンスの管理」の章を参照してください。

（注） 時間に対する列フィールドをプロットする各グラフを表示するには、列の下にある 0 以外の値をクリックします。

トラブルシューティング

1. **問題**：CVP ライセンスの使用率のダッシュレットに、「**使用可能なデータがありません（No Data Available）**」と表示される。

   推奨処置：次の条件が満たされていることを確認します。

   - CVP デバイスは、[インベントリ管理（Inventory Management）] で管理対象状態になっている必要があります。
   - CVP デバイスには、コール サーバ機能が必要です。

2. **問題**：CVP ライセンスの使用率のダッシュレットにエントリは表示されるが、ポート値が 0 として表示される、または変動する。

   推奨処置：CVP ライセンスの使用率のダッシュレットでは、ポーリングデータの時間間隔に基づいてエントリが表示されるため、ポート値は 0 として表示されるか、変動します。

Contact Center Enterprise ライセンスの使用状況

このダッシュレットには、Unified Contact Center Enterprise（(Unified CCE）ライセンスの使用状況が表示されます。

前提条件：

- Unified CCE Router または Unified CCE Peripheral Gateway は、[インベントリ管理（Inventory Management）] で管理対象状態になっている必要があります。
- Contact Center Assurance License が使用できる必要がある。

このダッシュレットには、過去 7 日間のポーリング レコードの最新カウントが表示されます。

次の詳細情報を表示できます。

- デバイス - デバイス名
- 機能 - ルータやペリフェラル ゲートウェイなどのデバイスの機能
- ログオン済みのエージェント - 現在ログオンしているエージェントの数

このダッシュレットには、ポーリングデータの時間間隔に基づいてエントリが表示されます。デフォルトのポーリング間隔は 1 分です。

Contact Center Assurance ライセンスの有効期限が切れると、Unified CCE ライセンス ダッシュレットは、Contact Center Enterprise ライセンスの使用状況を表示しません。この機能を継続して使用するには、必要な数の Cisco Prime Collaboration Contact Center の同時エージェント ライセンスを購入する必要があります。ライセンスの詳細については、ライセンスの管理の章を参照してください。

（注） 時間に対して列フィールドをプロットする各グラフを表示するには、**[ログオン済みのエージェント（Agents Logged On）]** 列で（0 以外の）値をクリックします。

トラブルシューティング

1. **問題**: Unified CCE ライセンス使用状況ダッシュレットに、**「使用可能なデータがありません（No Data Available）」**と表示されます。

   推奨処置：次の条件が満たされていることを確認します。

   - Unified CCE デバイスは、[インベントリ管理（Inventory Management）] で管理対象状態になっている必要があります。

- Unified CCE デバイスには、Unified CCE Router または Unified CCE PG 機能、あるいは両方が必要です。

2. **問題**：Unified CCE ライセンス使用状況ダッシュレットにエントリは表示されますが、**[ログオン済みエージェント（Agents Logged On）]** の値は 0 として表示されるか、継続的に変更します。

   推奨処置：Unified CCE ライセンス使用状況ダッシュレットは、ポーリング データの間隔に基づいたエントリを表示するため、**[ログオン済みエージェント（Agents Logged On）]** には 0 として表示されるか、値は継続的に変化します。

カスタマー サマリ ダッシュボード

カスタマー サマリ ダッシュボードを使用すると、エンドポイントやインフラストラクチャ デバイスの詳細情報、および特定のカスタマーのネットワークの論理的なトップレベル ビューを確認できます。

Cisco Prime Collaboration Assurance が MSP モードで展開されている場合は、Cisco Prime Collaboration Assurance ホーム ページから次のダッシュボードを表示できます。

ダッシュボード	説明
カスタマー サマリ	カスタマーごとのアラーム、エンドポイント、インベントリに関する情報。
Cisco Prime Collaboration リリース 11.1 以前の場合 TelePresence Exchange	クラスタ ノード、コールおよびセッション制御デバイス、リージョンの概要、および会議デバイスに関する情報。 （注） CTXデバイスが管理されていない場合は、どのダッシュレットにもデータは読み込まれません。

カスタマー サマリ ダッシュボードは、アラーム、エンドポイント、会議アラーム、およびインベントリに関する情報を、カスタマーごとに集約して提供します。次のダッシュレットが含まれています。

ダッシュレット	説明
アラームの概要	カスタマーごとのアラームの一覧を、重大度に基づいて表示します。各カスタマー レベルについて、重大度に基づく合計アラーム数が示されます。次の詳細情報を表示できます。 • 顧客 • Total • 重大 • やや重大 • 比較的重大でない • 警告
デバイスの概要	カスタマーごとのアラームの一覧を、重大度に基づいて表示します。各カスタマー レベルについて、重大度に基づく合計アラーム数が示されます。次の詳細情報を表示できます。 • 顧客 • Total • Managed • Unmanaged • Suspended
エンドポイントの概要	カスタマーごとに、各カテゴリのエンドポイントの一覧を、登録ステータスに基づいて表示します。次の詳細情報を表示できます。 • 顧客 • 合計：登録済み • 合計：未登録 • ハード エンドポイント：登録済み • ハード エンドポイント：未登録 • ソフト クライアント：登録済み • ソフト クライアント：未登録

ダッシュレット	説明
アラームの会議	アラームで進行中の会議の数を表示します。次の詳細情報を表示できます。 • 会議構造 • 会議タイプ • 監視された会議 • **Cisco Prime Collaboration リリース 11.1 以前の場合** トラブルシューティングのステータス • 会議の議題 • スケジューラの所属組織 • 開始時刻
音声コール品質イベントの概要（Voice Call Quality Events Summary）	アクティブなサービス品質（SQ）イベントの概要と、影響を受けるエンドポイントを表示します。過去 4 時間のアクティブな SQ イベント データと、影響を受けるエンドポイント数の概要が表示されます。

Contact Center Assurance ダッシュボード

Cisco Prime Collaboration Contact Center Assurance のパフォーマンス ダッシュボードは、Cisco Unified Intelligence Center（CUIC）、Finesse, MediaSense, Customer Voice Portal（CVP）、Unified Contact Center Enterprise（Unified CCE）、Unified Contact Center Express（Unified CCX）、Virtualized Voice Browser などの Contact Center のコンポーネントについてほぼリアルタイムの情報を提供することによって、ネットワークの監視をサポートします。

Finesse については、[System Summary]、[CPU and Memory]、[Disk Usage]、および [Process] ダッシュレットのみが表示されます。

（注） CUIC、Finesse、および MediaSense デバイスに対してクラスタリングが設定されている場合、ダッシュボードには、クラスタに属している関連デバイスのデータも表示されます。

Cisco Prime Collaboration Assurance が Enterprise モードで展開した場合、ダッシュボードを表示するには、 に移動します。**[監視（Monitor）]**>**[システム ビュー（System View）]**>**[パフォーマンス（Performance）]**[クラスタ（Cluster）] ドロップダウン リストから製品とクラスタを選択し、[ダッシュボード（Dashboard）] ドロップダウン リストから必要なダッシュボードを選択します。

Cisco Prime Collaboration Assurance を MSP モードで展開した場合、ダッシュボードを表示するには、[モニタ（Monitor）]>[システムビュー（System View）]>[カスタマー サマリ（Customer

Summary）] に移動し、顧客名をクリックして、[パフォーマンス（Performance）] をクリックします。[クラスタ（Cluster）] ドロップダウン リストから製品とクラスタを選択し、[ダッシュボード（Dashboard）] ドロップダウン リストから必要なダッシュボードを選択します。

Cisco Prime Collaboration リリース 11.5 以降の場合

エンタープライズ モードで Cisco Prime Collaboration Assurance を導入している場合は、ダッシュボードを表示するには、次のページを参照してください。 **[ネットワーク正常性の概要（Network Health Overview）] > [パフォーマンス（Performance）]**[クラスタ（Cluster）] ドロップダウン リストから製品とクラスタを選択し、[ダッシュボード（Dashboard）] ドロップダウン リストから必要なダッシュボードを選択します。

MSP モードで Cisco Prime Collaboration Assurance を導入している場合は、ダッシュボードを表示するには、次のページを参照してください。 **[ネットワーク正常性の概要（Network Health Overview）] > [カスタマー サマリ（Customer Summary）]**で、顧客の名前をクリックし、[パフォーマンス（Performance）]をクリックします。[クラスタ（Cluster）] ドロップダウン リストから製品とクラスタを選択し、[ダッシュボード（Dashboard）] ドロップダウン リストから必要なダッシュボードを選択します。

Cisco Prime Collaboration リリース 12.1 以降の場合

（注） エクスポートしたレポートの情報を表示するために、すべてのノードでクラスタを検出する必要があります。ポーリングは、検出されたノードに対してのみ行われます。

Contact Center Assurance トポロジ ダッシュボード

Cisco Prime Collaboration Assurance Advanced は、IP ベースの Contact Center の論理的なトップレベル ビューを提供します。ここには、Cisco Prime Collaboration Assurance で管理される Unified Contact Center デバイスが簡潔なトポロジで表示されます。

Contact Center のトポロジでは、IP ベースの Contact Center のデバイス セット全体を表示します。これはプライマリ データセンターとみなされ（トポロジではサイド A として表示）、プライベートおよびパブリック クラウドを介してセカンダリ データセンター（サイド B として表示）に接続されます。

Cisco Prime Collaboration Assurance が Enterprise モードで展開されている場合は、 に移動します。**[監視（Monitor）] > [システム ビュー（System View）] > [OpsView] > [Contact Center トポロジ（Contact Center Topology）]**。

Cisco Prime Collaboration リリース 11.5 以降の場合

エンタープライズ モードで Cisco Prime Collaboration Assurance を導入している場合は、 **[ネットワーク正常性の概要（Network Health Overview）] > [Contact Center トポロジ（Contact Center Topology）]**。

Cisco Prime Collaboration Assurance が MSP モードで展開されている場合、ダッシュボードには、Cisco Prime Collaboration Assurance で管理される、特定のカスタマーのすべてのデバイスが表示されます。[Contact Center Topology] ページに移動するには、ホームページでカスタマーをクリックします（[Customer Summary] > [Customer name]）。対象のカスタマーに対応するト

ポロジを表示するには、[Contact Center Topology] をクリックします。デバイスに対する管理対象の IP アドレスがトポロジ ビューに表示されます。

トポロジ内のクラウド（パブリックおよびプライベート クラウド）に対して、設定済みの対応するインターフェイス情報が表示されます。

カウンタに対するパフォーマンス ダッシュボードを新しいタブに表示するには、パフォーマンス カウンタの名前または（トポロジで各デバイス アイコンの下に表示される）値をクリックします。パフォーマンス ダッシュボードの詳細については、「カスタム パフォーマンス ダッシュボードの作成」を参照してください。

Contact Center Assurance のトポロジは、Contact Center 内のさまざまなデバイス間の関係に焦点をあてます。デバイスにマウス ポインタを合わせると、IP アドレスとホスト名の詳細が表示されます。Contact Center トポロジ ダッシュボードには次のデバイスが表示されます。

デバイスの一覧については、『Cisco Prime Collaboration Assurance でサポートされているデバイス』を参照してください。

Cisco Prime Collaboration リリース 11.6 以降の場合

次の表に、Unified Contact Center のデバイス間のリンク ステータスを示します。

デバイス 1	デバイス 2	リンク ステータス
IPCC	VRU PG	はい
IPCC	エージェント PG	はい
VRU PG	CVP コール サーバ	はい
CVP	VXML ゲートウェイ	いいえ
エージェント PG	CUCM	はい
CUCM	Media Sense	はい
エージェント PG	Finesse	はい
AW/HDS	CUIC	はい
UCCE ルータ	パブリック クラウド	はい
UCCE ルータ	プライベート クラウド	はい
UCCE ルータ	CTI	はい
CTI	CTIOS	はい
UCCE ルータ	MR PG	はい
VRU PG	CVP Reporting Server	いいえ
UCCE ルータ	ロガー	いいえ
UCCE ルータ	AW/HDS	はい
CVP	Virtualized Voice Browser（VVB）	いいえ

（注） Virtualized Voice Browser（VVB）が CVP バージョン 11.5 以降と統合されている場合は、Contact Center Assurance トポロジ内の VVB デバイスを表示できます。

[Select Any Router] ドロップダウン リストから Contact Center の導入用ルータ ペアを選択できます。選択したルータ ペアに対するトポロジが表示されます。インベントリからルータを削除すると、ドロップダウン リストには削除されたルータ、およびルータが属しているサイド（サイド A またはサイド B）はトポロジに表示されなくなります。

これは、Cisco Prime Collaboration Assurance が Enterprise モードで展開されている場合にのみ適用されます。

トポロジ ビューによるトラブルシューティング

Contact Center Assurance のトポロジ ビューでは、デバイスでアラームが生成されると、デバイスの隣にアラーム アイコンが表示されます。マウスをデバイスの IP アドレスに合わせると Device 360° ビューがクイック起動され、問題のトラブルシューティングにも役に立ちます。Device 360° ビューから、アラームおよびインターフェイスを確認することができます。また、トレース ルートを実行する、デバイスを ping する、[Alarms and Events] ページにアクセスする、といったことも可能です。Device 360° ビューの詳細については、『Cisco Prime Collaboration Assurance Guide - Advanced』の「「Managing Inventory」」の章を参照してください。

アラームが示されているデバイスには、アラームの最も高い重大度のみが表示されます。アラームが生成されると、そのアラームは消去されるまで Contact Center Assurance のトポロジ ビューに残ります。消去されたアラームは、Cisco Prime Collaboration Assurance の消去操作を呼び出した後に削除されます。

Cisco Prime Collaboration Assurance が MSP モードで展開されている場合、共有コンポーネントは共通の展開で管理されます。共有されるデバイスについては、IP アドレスのみ参照できます。共有されているデバイスへのアクセス権を持っていない場合は、それらのデバイスの Device 360° を起動できません（デバイスへのアクセス権を持っていないカスタマーに対しては、共有されているデバイスは表示専用モードになります）。

（注）
- Cisco Prime Collaboration Assurance が MSP モードで展開されている場合、共有（4 K Shared Contact Center）と専用の両方の導入モデルを管理している状況では、トポロジ ビューはサポートされません。
- トポロジ ビューは 2 分ごとに自動で更新されます。
- Cisco Prime Collaboration Assurance は、単一の Unified CCE エンタープライズ展開のみをサポートしています。
- 展開/縮小アイコンは、抽象デバイスでのみ使用できます。
- Unified CCE トポロジは、いずれかの側で複数のペリフェラル ゲートウェイ（PG）サーバが管理されている場合はサポートされません。トポロジを正しく起動するには、追加のペリフェラル ゲートウェイ（PG）をインベントリ管理から削除してください。

履歴トレンドの表示

履歴トレンド分析は、デフォルトで [System Summary] ダッシュボードの下位のダッシュレット（[CPU Usage]、[Virtual Memory Usage]、および [Common Partition Usage]）に対して有効になっています。トレンド ビュー グラフを表示するには、ダッシュレットの右下の [Zoom] をクリックします。

前提条件

すべてのデバイスが Cisco Prime Collaboration Assurance で管理対象状態になっている必要があります。クラスタの場合は、すべてのノードが管理対象状態になっている必要があります。

音声デバイス（Cisco Unified CM、Cisco Packaged Contact Center Enterprise、Cisco Unified Presence、Cisco Unity Connection、Cisco Media Sense、Cisco Finesse、Cisco Unified IC、および Cisco Unified Contact Center Express）の場合は、システム定義のダッシュボードと一緒に、デバイス関連のメトリックのトレンドも表示できます。

Cisco Prime Collaboration リリース 11.5 以降の場合

音声デバイス（Cisco Unified CM、Cisco Packaged Contact Center Enterprise、Cisco Unified Presence、Cisco Unity Connection、Cisco Media Sense、Cisco Finesse、Cisco Unified IC、Cisco Unified Contact Center Express、および Cisco Virtualized Voice Browser）の場合は、システム定義のダッシュボードと一緒に、デバイス関連のメトリックのトレンドも表示できます。

（注）
- デバイス関連のメトリックは、選択するデバイス タイプによって異なります。
- 履歴トレンド分析は、Cisco Unified CCE、Cisco Voice Portal、MCU/TPS、Cisco Unified Border Element、シスコ音声ゲートウェイ、Cisco Unified Communications Manager Express、ISDN ゲートウェイなどの非音声デバイスではサポートされていません。

[Trend] ダッシュボード

メトリックのトレンドを表示するには、[Dashboard] ドロップダウン リストから [Trend] を選択し、[Metrics Selection] ダイアログボックスからトレンドを有効にするメトリックを選択して [Add] をクリックします。任意の数のメトリックを選択できますが、デバイス タイプごとに最大 6 個までのメトリックを選択することをお勧めします。

また、次の操作を実行できます。

- データを、チャートまたは表形式のいずれかで表示する。
- [Merge] オプションをクリックして、2 つ以上のパフォーマンス メトリックについてトレンドを比較する。
- [Zoom] をクリックして、トレンド グラフを詳細ビューで表示する。このオプションは、履歴、1 時間ごとの平均、最大、および最小のデータを表示する場合に便利です。詳細ビューに表示されるズーム セレクタ グラフを使用して、選択した期間のトレンドを表示するためのグラフの時間枠（x 軸）のポインタを調整することができます。

- ユーザインターフェイスの右上にある [Add Graph]（+）ボタンを使用してトレンドを追加する。
- チャート タイプを変更する。

Customer Voice Portal（CVP）

Cisco Prime Collaboration Assurance には コール サーバ ベースの CVP ダッシュボードがあります。これはシステムで定義されており、Customer Voice Portal を追加するときに使用できます。また、モニタリングのニーズに基づいてカスタム ダッシュボードを作成することができます。パフォーマンス カウンタの詳細については、『Operations Guide for Cisco Unified Customer Voice Portal』を参照してください。

ダッシュボードを表示するには、 に移動します。**[モニタ（Monitor）]** > **[システム ビュー（System View）]** > **[パフォーマンス（Performance）]**[クラスタ（Cluster）] ドロップダウン リストから CVP とクラスタを選択し、[ダッシュボード（Dashboard）] ドロップダウン リストから必要なダッシュボードを選択します。選択したダッシュボードに関連する情報が別のダッシュレットに表示されます。各ダッシュレットには、サーバの詳細、現在の使用状況、および直前の 3 分間に受け取った最大値が表示されます。

（注） Cisco Prime Collaboration Assurance で CVP ダッシュボード用のデータを表示するには、Customer Voice Portal で Cisco CVP Call Server と Cisco CVP VXML サービスをオンにし、オペレーション コンソール（OAMP）上で CVP コール サーバの下位の ICM、SIP および IVR サブシステムを有効にします。

システム概要

メモリ合計、1 秒あたりのページ フォールト、処理件数、Cisco ICM ルータ コール、およびサービスに関する情報を表示します。

Available Bytes

プロセスまたはシステムへの割り当てで使用するためにすぐに利用できる物理メモリの量（バイト）を表示します。

Committed Bytes

コミットされた仮想メモリの量（バイト）を表示します。

Processor Time

プロセスの実行にかかる時間を、CPU がプロセスで使用したわずかな時間をすべて含めて表示します。

Threads

手順の単一シーケンスを表示します。プロセス（プログラムの実行インスタンス）は1つ以上のスレッドで構成されます。

Page Faults Per Second

1 秒あたりのページ フォールトの平均数を表示します。これは 1 秒間に失敗したページ数で測定されます。それぞれのフォールト動作で障害が発生するのは 1 ページのみで、ページ数はページのフォールト動作の数と同じになるためです。

コール サーバ ICM の集約統計

ルックアップ要求の合計、コールの合計数、スイッチ レッグの合計数、および VRU レッグを表示します。

Call Server Stats ICM Total Lookup Requests
システムの開始時間以降に Unified ICM アプリケーションへ送信された外部 Unified CVP VXML Server のコール ルーティング要求の合計数を表示します。外部 Unified CVP VXML Server 内で発生するコールでは、Unified ICM アプリケーションからのコール ルーティング指示が必要です。

Call Server Stats ICM Total Calls
後続の VRU 処理、および Contact Center エージェントへのルーティングのためにシステムの開始時間以降に Unified ICM アプリケーションが受信した新しいコールの合計数を表示します。

Call Server Stats ICM Total SIP Switch Legs
システムの開始時間以降に、Session Initiation Protocol（SIP）から ICM アプリケーションが受信した VoIP コールの数を表示します。

Call Server Stats ICM Total VRU Legs
システムの開始時間以降、Unified ICM アプリケーションから VRU 処理を受信したコールの数を表示します。VRU 処理には、事前に録音されたメッセージの再生が含まれており、カスタマーの要求を理解するために Caller Entered Digits（CED）や音声認識技術が必要になります。

コール サーバ ICM の間隔統計

ルックアップ要求、受信した新しいコール数、SIP スイッチ レッグ数、および VRU レッグを表示します。

Call Server Stats ICM Interval SIP Switch Legs
現在の間隔中に SIP から ICM アプリケーションが受信したコール数を表示します。Unified ICM アプリケーションは、Session Initiation Protocol（SIP）から発生した VoIP コールを承認します。

Call Server Stats ICM Interval Lookup Requests
現在の間隔中に Unified ICM アプリケーションへ送信された外部 Unified CVP VXML Server のコール ルーティング要求の数を表示します。外部 Unified CVP VXML Server 内で発生するコールでは、Unified ICM アプリケーションからのコール ルーティング指示が必要です。

Call Server Stats ICM Interval VRU Legs
Unified ICM アプリケーションから VRU 処理を受信中のコール数を表示します。VRU 処理には、事前に録音されたメッセージの再生が含まれており、現在の間隔でのカスタマーの要求を理解するために Caller Entered Digits（CED）や音声認識技術が必要になります。

Call Server Stats ICM Interval New Calls
後続の Voice Response Unit（VRU）処理、および Contact Center エージェントへのルーティングのために現在の間隔中に Unified ICM アプリケーションが受信した新しいコールの数を表示します。

コール サーバ ICM のリアルタイム統計

アクティブ コール、VRU レッグ、SIP スイッチ レッグ、およびルックアップ要求に関する情報を表示します。

Call Server Stats ICM Active VRU Legs

Unified ICM サーバから Voice Response Unit（VRU）処理を受信中の現在のコール数を表示します。VRU 処理には、事前に録音されたメッセージの再生が含まれており、カスタマーの要求を理解するために Caller Entered Digits（CED）や音声認識技術が必要になります。

Call Server Stats ICM Active SIP Switch Legs

SIP プロトコルから Unified ICM Server が受信したコール数を表示します。Active SIP Switch Legs は、Unified CVP Call Server から SIP プロトコルを使用して ICM Server が受信した現在のコールの数を表します。

Call Server Stats ICM Active Lookup Requests

ICM Server へ送信された外部 VXML Server コール ルーティング要求の現在の数を表示します。外部 Unified CVP VXML Server から発生するコールでは、Unified ICM Server からのコール ルーティング指示が必要です。

Call Server Stats ICM Active Calls

Unified CVP Call Server に対して ICM Server で処理されている現在のコール数を表示します。この値は、Contact Center エージェントへの後続のルーティングのために、Unified CVP Call Server に対して ICM で現在処理しているコールのカウントを表します。

コール サーバ インフラストラクチャ JVM のリアルタイム統計

使用中のリアルタイム JVM スレッド、メモリ合計、ピーク時のメモリ使用率、ピーク時のスレッド使用率、現在のメモリ使用率、および使用可能なメモリに関する情報が表示されます。

Call Server Stats RT JVM Threads In Use
Java 仮想マシンで現在使用されているスレッドの数を表示します。この数には、Unified CVP のスタンドアロンとスレッド プールのすべてのスレッド、および同じ JVM 内で実行中の Web アプリケーション サーバで作成されたスレッドが含まれています。

Call Server Stats RT JVM Total Mem
Java 仮想マシンで使用できるメモリの量（MB）を表示します。この数は、Java 仮想マシンに対してどのくらいのシステム メモリを使用できるかを表します。

Call Server Stats RT JVM Peak Mem Usage
起動してから Java 仮想マシンで使用されたメモリの最大量を表示します。報告される数はメガバイトの単位で、この Java 仮想マシンで同時に使用された、これまでで最大のメモリ量を表します。

Call Server Stats RT JVM Peak Threads
起動してから Java 仮想マシンで同時に使用されたスレッドの最大量を表示します。Java 仮想マシンで使用されたピーク時のスレッド数には、Unified CVP スタンドアロンとスレッド プールのすべてのスレッド、および同じ JVM 内で実行中の Web アプリケーション サーバで作成されたスレッドが含まれています。

Call Server Stats RT JVM Current Mem Usage
Java 仮想マシンで使用されている現在のメモリ（MB）を表示します。

Call Server Stats RT JVM Avail Mem
Java 仮想マシンで使用できるメモリの量を表示します。報告される数はメガバイト単位で、Java 仮想マシンで要求される現在のシステム メモリのうち、どのくらいが使用されていないかを表します。

コール サーバ インフラストラクチャ スレッド プールのリアルタイム統計

リアルタイムのアイドル プール スレッド数、使用されたスレッドの最大数、実行中のプール スレッド数、存在するスレッドの最大数、およびコア プール スレッドの統計を表示します。

Call Server Stats RT Idle Pool Threads
処理を待機しているアイドル状態のスレッドの数を表示します。

Call Server Stats RT Max Threads Used
処理を実行するように同時にタスクを割り当てられたスレッド プール スレッドの最大数を表示します。

Call Server Stats RT Running Pool Threads
処理を実行中のスレッド プールのスレッドの数を表示します。

Call Server Stats RT Max Threads
同時に存在するスレッド プールのスレッドの最大数を表示します。

Call Server Stats RT Core Pool Threads
アイドル状態がどんなに長くなっても絶対に破棄されないスレッドプールのスレッド数を表示します。

コール サーバ IVR の集約統計

1 秒間の間隔に取得される最大および平均の HTTP 要求、受信される HTTP 要求の合計、最大コール集約、および処理される HTTP の最大要求を表示します。

Call Server Stats IVR Max HTTP Req Sec Inter Aggregate Statistics

IVR サービスによって 1 秒間に同時に処理される HTTP 要求の現在の数を表示します。IVR サービスの開始以降に同時に処理されたアクティブな HTTP 要求の最大数。これは最高水準マーキングとも呼ばれます。

Call Server Stats IVR Max HTTP Requests Inter Aggregate Statistics

IVR サービスによって同時に処理される HTTP 要求の現在の数を表示します。

Call Server Stats IVR Avg HTTP Req Sec Inter Aggregate Statistics

IVR サービスによって 1 秒間に同時に処理される HTTP 要求の平均数を表示します。

Call Server Stats IVR Max Calls Agg

サービスの開始以降にIVRサービスによって同時に処理されたコールの最大数を表示します。

Call Server Stats IVR Total HTTP Req Agg

すべてのクライアントから受信したHTTP要求の数を表示します。このメトリックは、システムの開始以降に IVR サービスが受信した HTTP 要求の合計数です。

コール サーバ IVR のコール間隔統計

コールの終了間隔、最大コール間隔、最小コール遅延間隔、新しいコール間隔、平均コール遅延間隔、および最大コール遅延間隔の統計を表示します。

Call Server Stats IVR Calls Finished Inter

この間隔中に終了した Unified CVP コールの数を表示します。Call Finished メトリックのために、コールにはスイッチ レッグと Unified CVP コールの IVR レッグの両方が含まれます。コールの両方のレッグが終了すると、*Calls Finished* メトリックが増加します。

Call Server Stats IVR Max Calls Inter

この間隔の間に IVR サービスで同時に処理されたコールの最大数を表示します。

Call Server Stats IVR Min Call Latency Inter

IVR サービスが New Call Request または Request Instruction Request を処理するのにかかる最短の時間（ミリ秒）を表示します。

Call Server Stats IVR New Calls Inter

IOS ゲートウェイから受信した New Call 要求の数を表示します。New Call には、コールのスイッチレッグ、およびコールのIVRレッグが含まれています。このメトリックは、IVR サービスで受信する New Call Request の数をカウントします。

Call Server Stats IVR Avg Call Latency Inter

IVR サービスが New Call または Call Result Request を処理するのにかかる平均時間（ミリ秒）を表示します。

Call Server Stats IVR Max Call Latency Inter

IVR サービスが New Call Request または Request Instruction Request を処理するのにかかる最短の時間（ミリ秒）を表示します。

コール サーバ IVR の HTTP 間隔統計

1 秒間の間隔に取得される最大および平均の HTTP 要求と、最大およびアクティブな HTTP 要求の間隔統計を表示します。

Call Server Stats IVR Max HTTP Req Sec Inter

IVR サービスが 1 秒間にすべてのクライアントから受信する HTTP 要求の数を表示します。1 秒あたりのピーク HTTP 要求は、ある 1 秒間に IVR サービスが処理した HTTP 要求の最大数です。これは最高水準マーキングとも呼ばれます。

Call Server Stats IVR Max HTTP Requests Inter
この時間間隔においてIVRサービスがクライアントから受信したHTTP要求の最大数を表示します。

Call Server Stats IVR Avg HTTP Req Sec Inter
IVR サービスが 1 秒間に受け取る HTTP 要求の平均数を表示します。

Call Server Stats IVR Active HTTP Requests Inter
IVR サービスによって同時に処理されているHTTP要求の現在の数を表示します。ピークアクティブ要求は、この時間間隔においてIVRサービスが同時に処理しているHTTP要求の最大数を表すメトリックです。

コール サーバ IVR のリアルタイム統計

IVR のアクティブ コールおよびアクティブな HTTP 要求の統計を表示します。

Call Server Stats IVR Active Calls
IVR サービスによって処理されているアクティブ コールの数を表示します。

Call Server Stats IVR Active HTTP Requests
IVR サービスによって処理されているアクティブ HTTP 要求の数を表示します。

コール サーバ SIP エージェントのグリーティング集約統計

応答されたグリーティングの合計、および失敗したグリーティングの合計を表示します。

Call Server Stats SIP Total Greeting Answered

システムの開始時間以降に、エージェントのグリーティングが成功したコールの合計数を表示します。

Call Server Stats SIP Total Greeting Failed

システムの開始時間以降に、エージェントのグリーティングが失敗したコールの合計数を表示します。

コール サーバ SIP エージェントのグリーティング間隔統計

応答された間隔グリーティング、および失敗した間隔グリーティングの統計を表示します。

Call Server Stats SIP Int Greeting Answered

間隔中にエージェント グリーティングが成功したコールの数を表示します。

Call Server Stats SIP Int Greeting Failed

間隔中にエージェント グリーティングが失敗したコールの数を表示します。

コール サーバ SIP の集約統計

最初および 2 回目の集約の平均 LAT、集約前後に失敗した XFR、集約後に受信した接続、および NC subs の集約統計に関する情報を表示します。

Call Server Stats SIP Avg LAT Second Agg

2 回目以降の転送で応答されたコールの平均遅延の計算が表示されます。

Call Server Stats SIP Fail XFR Post Agg

開始時間以降にコールの受信または送信レッグで失敗した再招待要求の数を表示します。再招待メッセージは、SIP ダイアログが確立された後で転送を実行します。再招待の要求は、エンドポイントから発生するか、または Unified CVP 転送によって Unified ICME スクリプトから開始されます。このカウンタには、再招待要求の失敗が含まれます。

Call Server Stats SIP Conn Recpt Post Agg

システムの開始時間以降、Unified CVP の転送を実行するために SIP サービスで受信した Connect メッセージの数を表示します。Connects Received には、通常の Unified CVP の転送と Refer の転送が含まれています。ICM サービスから生じるラベルは、VRU へ送信されるものでも、エージェントへ転送されるものでも、Connect メッセージになります。

Call Server Stats SIP Avg LAT First Agg

最初の転送で応答されたコールの平均遅延の計算が表示されます。

Call Server Stats SIP Fail XFR Pre Agg

システムの開始時間以降、最初の CVP 転送で失敗した転送の合計数を表示します。最初の CVP 転送が終了した後で SIP ダイアログが確立されます。メトリックには、SIP のサービス停止による拒否は含まれません。メトリックには、CONNECT メッセージにおいて ICM からラベルが返された後で失敗した転送も含まれます。

Call Server Stats SIP NC Subs Agg

システムの開始時間以降、Unified CVP で受信した SIP Invite メッセージの数を表示します。これには、失敗したコール、SIP サービスが使用不可であるために拒否されたコールも含まれます。

コール サーバ SIP 間隔統計

接続が受信された間隔、NC subs の間隔、平均 LAT 秒間隔、失敗した XFR の間隔の前後、コール後に応答した間隔の統計を表示します。

Call Server Stats SIP Conn Recpt Inter

最後の統計集約の間隔で、Transfer をコールするために SIP サービスが受信した CONNECT メッセージの数を表示します。Connects Received には、通常の Unified CVP の転送と Refer の転送が含まれています。ICM サービスから生じるラベルは、VRU へ送信されるものでも、エージェントへ転送されるものでも、CONNECT メッセージと見なされます。

Call Server Stats SIP NC Subs Inter

現在の間隔において Unified CVP が受信した SIP Invite メッセージの数を表示します。これには、失敗したコール、SIP サービスが使用不可であるために拒否されたコールも含まれます。

Call Server Stats SIP Avg LAT Second Inter

ICM から CONNECT が発信されたときから、コールに応答されるまでの時間を表示します。メトリックには、最後の統計集約間隔で応答されたコールの平均遅延の計算が含まれます。

Call Server Stats SIP Int Post Call Answered

間隔中に応答されたサービス コールの数を表示します。

Call Server Stats SIP Fail XFR Post Inter

間隔中にコールの受信または送信レッグのいずれかにおいて失敗した再招待要求の数を表示します。再招待メッセージは、SIP ダイアログが確立された後で転送を実行します。再招待の要求は、エンドポイントから発生するか、または Unified CVP 転送によって Unified ICME スクリプトから開始されます。このカウンタには、両方の種類の再招待要求の失敗が含まれます。

Call Server Stats SIP Fail XFR Pre Inter

システムの開始時間以降、失敗した SIP 転送の数を表示します。Unified CVP がコールの最初の宛先へ転送しようとする場合、最初の INVITE 要求を送信して、ICM へルーティングされている宛先ラベルを発信者に設定します。メトリックには、SIP サービスが実行されていないことによる拒否は含まれません。メトリックには、CONNECT メッセージにおいて ICM Server からラベルが返された後で失敗した転送も含まれます。

コール サーバ SIP リアルタイム統計

グリーティング コール、アクティブ コール、ウィスパー コール、およびコールの合計の数を表示します。

Call Server Stats SIP Greeting Calls

SIP サービスが処理するグリーティング コールの合計数を表示します。

Call Server Stats SIP Active Calls

SIP サービスが処理中のコールの件数を表すリアルタイムのスナップショット メトリックを表示します。

Call Server Stats SIP Whisper Calls

SIP サービスが処理するウィスパー コールの合計数を表示します。

Call Server Stats SIP Total Calls

SIP サービスが処理中のコールの合計数を表示します。メトリックには、着信、発信、および呼び出し音のタイプのコールが含まれます。SIP サービスの各アクティブ コールには、転送ラベルの宛先に対する着信コールと発信コールがあります。

コール サーバ SIP ウィスパー アナウンスメントの間隔統計

応答された間隔ウィスパー、および失敗した間隔ウィスパーの統計を表示します。

Call Server Stats SIP Int Whisper Failed

間隔中にウィスパー アナウンスメントが失敗したコールの数を表示します。

Call Server Stats SIP Int Whisper Answered

間隔中にウィスパー アナウンスメントが成功したコールの数を表示します。

コール サーバ SIP ウィスパー アナウンスメントの統計

応答されたウィスパーの合計、および失敗したウィスパーの合計を表示します。

Call Server Stats SIP Total Whisper Answered

システムの開始時間以降にウィスパー アナウンスが成功したコールの合計数を表示します。

Call Server Stats SIP Total Whisper Failed

システムの開始時間以降に、ウィスパーアナウンスメントが失敗したコールの合計数を表示します。

VXML インフラストラクチャ JVM メモリのリアルタイム統計

JVM で利用可能なリアルタイムのメモリ、メモリ合計、現在のメモリ使用状況、稼働時間、およびピーク時のメモリ使用率に関する情報を表示します。

VXML Server Stats RT JVM Avail Mem

Java 仮想マシンで使用できるメモリの量を表示します。報告される数はメガバイト単位で、Java 仮想マシンで要求される現在のシステム メモリのうち、どのくらいが使用されていないかを表します。

VXML Server Stats RT JVM Total Mem

Java 仮想マシンで使用できるメモリの量（MB）を表示します。この数は、Java 仮想マシンに対してどのくらいのシステム メモリを使用できるかを表します。

VXML Server Stats RT JVM Current Mem Usage

Java 仮想マシンで使用されている現在のメモリ（MB）を表示します。

VXML Server Stats RT JVM Uptime

Java 仮想マシンが稼働した時間を表示します。この時間は hh:mm:ss で測定され、Java 仮想マシンのプロセスが開始されてから経過した時間を表します。

VXML Server Stats RT JVM Peak Mem Usage

起動してから Java 仮想マシンで使用されたメモリの最大量を表示します。報告される数はメガバイトの単位で、この Java 仮想マシンで同時に使用された、これまでで最大のメモリ量を表します。

VXML インフラストラクチャ JVM スレッドのリアルタイム統計

現在使用されているスレッドの数と、Java 仮想マシンで同時に使用されたピークのスレッド数を表示します。

VXML Server Stats RT JVM Threads in Use

Java 仮想マシンで現在使用されているスレッドの数を表示します。この数には、Unified CVP のスタンドアロンとスレッド プールのすべてのスレッド、および同じ JVM 内で実行中の Web アプリケーション サーバで作成されたスレッドが含まれています。

VXML Server Stats RT JVM Peak Threads

起動してから Java 仮想マシンで同時に使用されたスレッドの最大量を表示します。Java 仮想マシンで使用されたピーク時のスレッド数には、Unified CVP スタンドアロンとスレッド プールのすべてのスレッド、および同じ JVM 内で実行中の Web アプリケーション サーバで作成されたスレッドが含まれています。

VXML インフラストラクチャ スレッド プールのリアルタイム統計

リアルタイムのアイドル プール スレッド、コア プール スレッド、使用された最大スレッド、実行プール スレッド、および最大スレッドの統計を表示します。

VXML Server Stats RT Idle Pool Threads
処理を待機しているアイドル状態のスレッドの数を表示します。

VXML Server Stats RT Core Pool Threads
アイドル状態がどんなに長くなっても絶対に破棄されないスレッドプールのスレッド数を表示します。

VXML Server Stats RT Max Threads Used
処理を実行するように同時にタスクを割り当てられたスレッド プール スレッドの最大数を表示します。

VXML Server Stats RT Running Pool Threads
処理を実行中のスレッド プールのスレッドの数を表示します。

VXML Server Stats RT Max Threads
同時に存在するスレッド プールのスレッドの最大数を表示します。

VXML サーバの集約統計

セッションの集約合計、ルックアップの成功集約、ルックアップの応答集約、ルックアップの失敗集約、ルックアップの要求集約、およびレポート イベントの集約統計を表示します。

VXML Server Stats Total Sessions Agg
起動後の Unified CVP VXML サーバ内のセッション数を表示します。

VXML Server Stats ICM Lookup Successes Agg
起動後の Unified CVP VXML サーバから ICM Service への要求の数を表示します。ICM ルックアップ要求が成功するたびに、このメトリックが 1 だけ増加します。

VXML Server Stats ICM Lookup Responses Agg
起動後に ICM Service が Unified CVP VXML サーバへ送信した応答の数を表示します。1 つの ICM ルックアップ要求につき（成功、失敗のいずれの場合でも）、このメトリックが 1 だけ増加します。1 つの要求に対して複数の応答メッセージが Unified CVP VXML サーバへ送信された場合、このメトリックは ICM Service からの応答メッセージごとに増加します。

VXML Server Stats ICM Lookup Failures Agg
起動後の Unified CVP VXML サーバから ICM Service への要求の数を表示します。ICM ルックアップ要求が失敗するたびに、このメトリックが 1 だけ増加します。このメトリックは、ICM 失敗のメッセージが受信された場合、または Unified CVP VXML サーバで失敗メッセージを生成した場合に増加します。

VXML Server Stats ICM Lookup Requests Agg
Unified CVP VXML サーバから ICM Service への要求の数を表示します。1 つの ICM ルックアップ要求につき（成功、失敗のいずれの場合でも）、このメトリックが 1 だけ増加します。

VXML Server Stats Reporting Events Agg
起動後の Unified CVP VXML サーバから送信されたレポート イベントの数を表示します。

VXML サーバの間隔統計

レポートイベントの間隔、ルックアップの成功間隔、ルックアップの要求間隔、ルックアップの応答間隔、ルックアップの失敗間隔、およびセッション間隔の統計を表示します。

VXML Server Stats Reporting Events Inter
Unified CVP VXML サーバから Reporting Server へ送信されたイベントの数を表示します。

VXML Server Stats ICM Lookup Success Inter
現在の間隔で Unified CVP VXML サーバから ICM Service への成功した要求の数を表示します。

VXML Server Stats ICM Lookup Request Inter
Unified CVP VXML サーバから ICM Service への要求の数を表示します。

VXML Server Stats ICM Lookup Responses Inter
ICM Service が Unified CVP VXML サーバへ送信した、失敗および成功の ICM ルックアップ要求への応答の数を表示します。1 つの要求に対して複数の応答メッセージが Unified CVP VXML サーバへ送信された場合、このメトリックは ICM Service からの応答メッセージごとに増加します。

VXML Server Stats ICM Lookup Failure Inter
現在の間隔で Unified CVP VXML サーバから ICM Service への要求の数を表示します。このメトリックは、ICM 失敗のメッセージが受信された場合、または Unified CVP VXML サーバで失敗メッセージを生成した場合に増加します。

VXML Server Stats Session Inter
Unified CVP VXML サーバ内のセッション数を表示します。

VXML サーバのリアルタイム統計

アクティブな ICM ルックアップ要求の数およびアクティブ セッションの統計を表示します。

VXML Server Stats Active ICM Lookup Requests
現在 Unified CVP VXML サーバが処理している ICM 要求の数を表示します。

VXML Server Stats VXML Active Sessions
現在 Unified CVP VXML サーバが処理しているセッションの数を表示します。

Unified Contact Center Enterprise（Unified CCE）

Cisco Prime Collaboration Assurance には Unified CCE ダッシュボードがあります。これはシステムで定義されており、Unified CCE を追加するときに使用できます。また、モニタリングのニーズに基づいてカスタム ダッシュボードを作成することができます。パフォーマンス カウンタの詳細については、『Serviceability Best Practices Guide for Cisco Unified ICM/Contact Center Enterprise』を参照してください。

ダッシュボードを表示するには、 に移動します。**[モニタ（Monitor）]** > **[システム ビュー（System View）]** > **[パフォーマンス（Performance）]**[クラスタ（Cluster）] ドロップダウン リストから CCE とクラスタを選択し、[ダッシュボード（Dashboard）] ドロップダウン リストから必要なダッシュボードを選択します。選択したダッシュボードに関連する情報が別のダッシュレットに表示されます。各ダッシュレットには、サーバの詳細、現在の使用状況、および直前の 3 分間に受け取った最大値が表示されます。

（注） データを Cisco Prime Collaboration Assurance の Unified CCE で表示するには、Unified Contact Center Enterprise が機能している必要があります。

システム概要

メモリ合計、1 秒あたりのページ フォールト、処理件数、Cisco ICM ルータ コール、およびサービスに関する情報を表示します。

Total Memory

システム上の仮想メモリの使用率の合計量を表示します。

Page Faults Per Second

1 秒あたりのページ フォールトの平均数を表示します。これは 1 秒間に失敗したページ数で測定されます。それぞれのフォールト動作で障害が発生するのは 1 ページのみで、ページ数はページのフォールト動作の数と同じになるためです。

Handle Count

このプロセスによって現在オープンしているハンドルの合計数を表示します。この数は、対象プロセスの各スレッドによって現在オープンしているハンドルの合計と同じです。

Cisco ICM Router Calls

1 秒間に受信したコールの数で測定された、（算出された）着信コール レートを表示します。

Services

サービスの名前、ステータス（サービスが起動しているか、ダウンしているか、管理者によってアクティブ化されたか、停止されたか、開始しているか、停止しているか、または不明な状態か）、およびサーバ、または（該当する場合は）クラスタ内の特定のサーバのサービスが特定の状態にある間に経過した時間を表示します。

CTI SVR エージェントのステータス

待受中および待受停止のエージェント カウント、ログインおよびログアウトのエージェント カウント、通話中のエージェント カウント、および後処理後待受停止エージェント カウントを表示します。

Ready Agent Count

ログインしており、コールを受け取る準備ができているエージェントの数を表示します。

Work Not Ready Agent Count

最後のコールに関連付けられている処理を実行中のエージェント。このエージェントは、コールに接続されないことを意味します。これらのエージェントは、この状態を終了しても、追加のコールを受け取るための準備ができていません。

Not Ready Agent Count

ログインしているけれども、着信コールの受け取り以外のタスクを実行中であるエージェントの数を表示します。

Logged In Agent Count

ログインしたエージェントを表示します。これらのエージェントがコールの受け取り準備ができていることを示しているとは限りません。

Talking Agent Count

着信または発信のコールを実行中のエージェントの数を表示します。

Logged Out Agent count

システムからログアウトしたエージェントの数を表示します。この数は、何らかの状態の不一致が発生して統計を検証する場合に役に立ちます。

CTI SVR のセッション ステータス

クローズしたセッション、失敗したセッション、不明なセッション、オープンしたセッション、セッションの合計、およびオープンしているセッションを表示します。

Sessions Closed

CTI Server によって終了したセッションの合計数を表示します。

Sessions Failed

ハートビートが見つからない、オープン要求のタイムアウト、セッションが活動していない、などのさまざまな理由で失敗したセッションの数を表示します。これらのタイマーは、CTI Server で設定可能なパラメータです。

Sessions Unknown

ソケットがまだ接続されていないセッションの数を表示します。

Sessions Open

正常にセットアップされたセッションの数を表示します。

Total Sessions

CTI Server によって保持されているセッションの合計数を表示します。

Sessions Opening

接続の設定中であるセッションの数を表示します。

CTI SVR コール カウント

アクティブ コール カウント、プライベート コール カウント、クリアしたコール カウント、およびアクティブではないコール カウントを表示します。

Active Call Count

現在進行中のコールの数を表示します。

Private Call Count

CTI Server によって非公開で追跡され、OPC にはレポートされないコールの数を表示します。

Cleared Call Count
システムにはすでに存在していないコールの数を表示します。

Deactivated Call Count
現在アクティブではなく、最終的にクリアされるコールの数を表示します。

EAPIM コールとメッセージ数

1 秒間のコール、1 秒間のメッセージ、無効なコール数、エージェント数、コール数、および送信されたメッセージを表示します。

Calls Per Sec

1 秒あたりの着信コールの数を表示します。

Messages Per Sec

コール イベントの数、1 秒間に JTAPI Gateway と CM PIM 間で交換されたエージェント イベントの数を表示します。

Invalid Call Count

有効なコール状態のいずれにも該当しないコールの数を表示します。

Agent Count

システムで現在設定されているエージェントの数を表示します。

Call Count

進行中のコールの数を表示します。

Messages Sent

今日送信されたコールイベントの数、エージェントイベントの数、およびCSTAメッセージの数を表示します。

OPC SideA エージェント カウント

sideA エージェント カウント、後処理後待受および後処理後待受停止の sideA エージェント カウント、待受中および待受停止の sideA エージェント カウント、および通話中の sideA エージェント カウントを表示します。

Work Not Ready SideA Agent Count

最後のコールに関連付けられている処理を実行中のエージェントを表示します。このエージェントは、コールに接続されないことを意味します。これらのエージェントは、この状態を終了しても、追加のコールを受け取るための準備ができていません。

Ready SideA Agent Count

ログインしており、コールを受け取る準備ができているエージェントの数を表示します。

Not Ready SideA Agent Count

ログインしているけれども、着信コールの受け取り以外のタスクを実行中であるエージェントの数を表示します。

Talking SideA Agent Count

着信または発信のコールを実行中のエージェントの数を表示します。

SideA Agent Count

システムに設定されているエージェントの数を表示します。

Work Ready SideA Agent Count

最後のコールに関連付けられている処理を実行中のエージェントを表示します。これは、このエージェントは現在コールに接続されていませんが、この状態が終了したら、追加のコールを受け取ることができることを表しています。

OPC コール カウント

呼び出し中のコール カウント、失敗したコール カウント、コール カウント、キューイング中のコール カウント、接続されているコール カウント、および開始されたコール カウントを表示します。

OPC Alerting Call Count

デバイスが呼び出し中（音が鳴っている）状態のコールの数を表示します。これは、コールがデバイスへの接続を要求していることを表します。

OPC Failed Call Count

正常な状態の進行が中断されたコールの数を表示します。この状態は通常、デバイスがコールに接続しようとした、またはコールがデバイスに接続しようとした場合に失敗した状況を表します。発信側のデバイスおよびコールへの接続が失敗した、着信側のデバイスおよびコールへの接続が失敗した、コールの作成に失敗した、またはその他の理由が失敗の原因として考えられます。

OPC Call Count

現在アクティブなコールの数を表示します。

OPC Queued Call Count

正常な状態の進行が中断しているコールの数を表示します。この状態は通常2つの状態を表しますが、他にも当てはまる場合があります。1つは、デバイスがコールとの接続を確立しようとしてプロセスが中断されている状態です。もう1つは、コールがデバイスとの接続を確立しようとしてプロセスが中断されている状態です。

OPC Connected Call Count

デバイスがアクティブに参加しているコールの数を表示します。

OPC Initiated Call Count

デバイスがサービスを要求したコールの数を表示します。ほとんどの場合は、これはダイヤル中の状態です。

OPC SideA スキル グループおよびサービス カウント

スキル グループのカウントとサービス カウントを表示します。

OPC Skill Group Count

共通のスキルセットを共有しているため、すべてのエージェントが特定のタイプのコールを処理できるエージェントのグループを表示します。各スキル グループには 1 つ以上のエージェントが含まれます。ペリフェラルでサポートされている場合、各エージェントは複数のスキル グループのメンバーになることも可能です。このカウンタは、エージェントがサインインで使用できるさまざまなスキル グループの数を表します。

OPC Service Count

コールを処理するよう設定されているサービスの数を表示します。サービスは、発信側が必要とする処理のタイプです。ペリフェラルには、販売、テクニカルサポート、または新しいアカウントを開くために定義されたサービスが付属していることがあります。各サービスには1つ以上のスキル グループがあり、それらのグループのメンバーがサービスを提供できます。各スキル グループは複数のサービスに関連付けることが可能です。

VRUPIM のコールおよびメッセージ カウント

VRUPIM の新しいコール、ルーティング前のコール、VRU でのコール、VRU へのメッセージ、VRU からのメッセージ、および接続のリセット カウントを表示します。

VRUPIM New Calls

新しいコールが Voice Response Unit（VRU）に到達するレートを表示します。新しいコールは、サービス コントロール VRU に到達した時点で ICM スクリプトの制御下にはないコールになります。

VRUPIM Pre Routed Calls

ルーティング前のコールが VRU に到達するレートを表示します。ルーティング前のコールは、サービス コントロール VRU に到達した時点で ICM スクリプトの制御下のコールになります。

VRUPIM Calls at VRU

現在 VRU にあるコールの数を表示します。コール ルーティング インターフェイスのみを使用する VRU では、この値はゼロになります。

VRUPIM Messages To VRU

メッセージが VRU へ送信されるレートを表示します。このカウンタは、ICM レジストリで有効になっている場合のみアクティブになります。

VRUPIM Messages From VRU

VRU からメッセージが受信されたレートを表示します。このカウンタは、ICM レジストリで有効になっている場合のみアクティブになります。

VRUPIM Connection Resets

ICM と Voice Response Unit 間の TCP 接続が、アプリケーションの開始以降に、確立された状態からクローズされた状態へ変更された回数を表示します。

ICM ルータ コールのステータス

ルータ内のコール数、ルータのコール数、キュー内のコール数、および進行中のコール数を表示します。

ICM Router Calls in Router

ルータ内のアクティブなコールの数を表示します（処理のために VRU へ送信されたコールやキューイング中のコール、およびルータがルーティング クライアントからの応答を待機しているコールも含まれます）。

ICM Router Calls

1 秒間に受信したコールの数で測定された、（算出された）着信コール レートを表示します。

ICM Router Calls In Queue

すべてのネットワークの Voice Response Unit（VRU）内でキューイング中のコールの数を表示します。これはルータから見ると、キューイングのために VRU へ転送中であるコールも含まれます。

ICM Router Calls In Progress

進行中の（CCE アプリケーションで制御されている）コールの数を表示します。

ICM ルータ ステータス

ルータの拒否率、ルータのサイズ（KB）、処理されたメッセージ、最大および平均の処理時間、および輻輳レベルを表示します。

ICM Router Rejection Percentage

コール レートが高いために拒否されたコールの数を表示します。

ICM Router State Size in KB

現在のルータ状態のサイズ（ルータ メモリ内のすべての状態の転送オブジェクトの合計サイズ）を表示します。このサイズはキロバイトで測定されます。一方のルータ サイドでサービスが停止して、そのルータ サイドがインサービスを返すと、サービスが持続中のルータ サイドからインサービスを返したルータ サイドへルータの状態が転送されます。

ICM Router Messages Processed

ルータが処理した MDS メッセージの数を表示します。デフォルトでは、このカウンタは無効になっています。

ICM Router Max Process Time in ms

ルータが MDS メッセージの処理にかけた最大時間（ミリ秒）を表示します。

ICM Router Avg Process Time

ルータが MDS メッセージの処理にかけた平均時間を表示します。

ICM Router Congestion Level

コール レートが高いためにキューイングされた、またはブロックされたコールの数を表示します。

ICM ロガー DB の書き込み

書き込みの平均時間、処理された書き込みレコード、およびDB 書き込みの数を表示します。

ICM Logger Number of DB Write

履歴ロガープロセスにおけるデータベースの書き込み（レコード/行）の数を表示します。これは、カウンタがポーリングされたときにデータベースに書き込まれているものです。

ICM Logger DB Write Average Time

中央コントローラのデータベース内のテーブルにデータを書き込むために必要な平均時間（100 ナノ秒単位）を表示します。この値は、過去の 1 秒間に発生した書き込み処理において、1回の書き込みにかかる平均時間を表します。この値は、データベースアクセスの競合に対する優れた指標となります。

ICM Logger DB Write Records Processed

過去の 1 秒間に Historical Logger Process で処理された（データベースに書き込まれた）レコードの数を表示します。

ICM ディストリビュータのリアルタイム エージェント キュー

エージェント キューの深さ、スキル グループのキューの深さ、エージェント DB の書き込み平均時間と処理された書き込みレコード、および処理されたエージェントスキル グループ DB の書き込みレコードと書き込み平均時間を表示します。

ICM Distributor Real Time Agent Queue Depth

Real-time Client プロセスの Agent テーブルに対するキューの深さ（保留中の書き込みトランザクションの数）を表示します。

ICM Distributor Real Time Agent Skill Group Queue Depth

Real-time Client プロセスの Agent Skill Group テーブルに対するキューの深さ（保留中の書き込みトランザクションの数）を表示します。

ICM Distributor Real Time Agent DB Write Records Processed

過去の 1 秒間の間隔に Real-time Client プロセスによって書き込まれた Agent テーブルのレコード数を表示します。

ICM Distributor Real Time Agent DB Write Average Time

過去の 1 秒間の間隔に Real-time Client プロセスが Agent テーブルのトランザクションの書き込みを処理した平均時間（100 ns 単位）。

ICM Distributor Real Time Agent Skill Group DB Write Average Time

過去の 1 秒間の間隔に Real-time Client プロセスが Agent Skill Group テーブルのトランザクションの書き込みを処理した平均時間（100 ns 単位）。

ICM Distributor Real Time Agent Skill Group DB Write Records Processed

過去の 1 秒間の間隔に Real-time Client プロセスによって書き込まれた Agent Skill Group テーブルのレコード数を表示します。

ディストリビュータのリアルタイム ルート DB の書き込み

処理された書き込みレコードの数、キューの深さ、およびルートテーブルの書き込みトランザクションにかかった平均時間を表示します。

ICM Distributor Real Time Route DB Write Average Time

過去の 1 秒間の間隔に Real-time Client プロセスが Route テーブルのトランザクションの書き込みを処理した平均時間（100 ns 単位）。

ICM Distributor Real Time Route DB Write Records Processed

過去の 1 秒間の間隔に Real-time Client プロセスによって書き込まれた Route テーブルのレコード数を表示します。

ICM Distributor Real Time Route Queue Depth

Real-time Client プロセスの Route テーブルに対するキューの深さ（保留中の書き込みトランザクションの数）を表示します。

ディストリビュータのリアルタイム サービス DB の書き込み

サービス DB の処理された書き込みレコード、キューの深さ、および平均時間を表示します。

ICM Distributor Real Time Service DB Write Records Processed

過去の 1 秒間の間隔に Real-time Client プロセスによって書き込まれた Service テーブルのレコード数を表示します。

ICM Distributor Real Time Service Queue Depth

Real-time Client プロセスの Service テーブルに対するキューの深さ（保留中の書き込みトランザクションの数）を表示します。

ICM Distributor Real Time Service DB Write Average Time

過去の 1 秒間の間隔に Real-time Client プロセスが Service テーブルのトランザクションの書き込みを処理した平均時間（100 ns 単位）。

ディストリビュータのリアルタイム スキル グループ DB の書き込み

スキル グループの処理された書き込みレコード、平均時間、およびキューの深さを表示します。

ICM Distributor Real Time Skill Group DB Write Records Processed

過去の 1 秒間の間隔に Real-time Client プロセスによって書き込まれた Skill Group テーブルのレコード数を表示します。

ICM Distributor Real Time Skill Group Queue Depth

Real-time Client プロセスの Skill Group テーブルに対するキューの深さ（保留中の書き込みトランザクションの数）を表示します。

ICM Distributor Real Time Skill Group DB Write Average Time

過去の 1 秒間の間隔に Real-time Client プロセスが Skill Group テーブルのトランザクションの書き込みを処理した平均時間（100 ns 単位）。

ディストリビュータのリアルタイム コールタイプ DB の書き込み

コールタイプ DB の平均書き込み時間、処理されたレコード、およびキューの深さを表示します。

ICM Distributor Real Time Call Type DB Write Average Time

過去の 1 秒間の間隔に Real-time Client プロセスが CallType テーブルのトランザクションの書き込みを処理した平均時間（100 ns 単位）。

ICM Distributor Real Time Call Type DB Records Processed

過去の 1 秒間の間隔に Real-time Client プロセスによって書き込まれた CallType テーブルのレコード数を表示します。

ICM Distributor Real Time Call Type Queue Depth

Real-time Client プロセスの CallType テーブルに対するキューの深さ（保留中の書き込みトランザクションの数）を表示します。

ディストリビュータの Replication DB の書き込み

ディストリビュータのレプリケーション DB の平均時間および処理されたレコード数を表示します。

ICM Distributor Replication DB Write Average Time
過去の 1 秒間の間隔における HDS Replication プロセスのデータベース書き込み処理の平均時間（100 ns 単位）。

ICM Distributor Replication DB Records Processed
過去の 1 秒間の間隔に HDS Replication プロセスによって書き込まれたレコード数を表示します。

Cisco Unified Intelligence Center

Cisco Prime Collaboration Assurance には、システムで定義された Cisco Unified Intelligence Center のダッシュボードがあり、Cisco Unified Intelligence Center を追加すると使用可能になります。Cisco Prime Collaboration Assurance では、モニタリングのニーズに基づいてカスタム ダッシュボードを作成することができます。パフォーマンス カウンタの詳細については、『Cisco Unified Intelligence Center 用管理コンソール ユーザ ガイド』を参照してください。

ダッシュボードを表示するには、 に移動します。**[モニタ（Monitor）]** > **[システム ビュー（System View）]** > **[パフォーマンス（Performance）]**と選択し、[クラスタ（Cluster）] ドロップダウン リストから [インテリジェンス センタ（Intelligence Center）] とクラスタを選択して、[ダッシュボード（Dashboard）] ドロップダウン リストから必要なダッシュボードを選択します。選択したダッシュボードに関連する情報が別のダッシュレットに表示されます。各ダッシュレットには、サーバの詳細、現在の使用状況、および直前の 3 分間に受け取った最大値が表示されます。

前提条件：

- Cisco Unified Intelligence Center が Cisco Prime Collaboration Assurance で管理されている必要があります。

- Cisco Prime Collaboration Assurance で Cisco Unified Intelligence Center のダッシュボードにデータが表示されるようにするには、Cisco Unified Intelligence Center バージョン 9.x 以降に到達できる必要があります。

次に、Cisco Unified Intelligence Center の新しくサポートされるダッシュボードを示します。

システムの要約

CPU 使用率、仮想メモリ使用率、共通パーティションの使用率、重要なサービス ステータスに関する情報を表示します。システム管理者は、[システムの概要（System Summary）] ダッシュレットをモニタして、システムの応答の遅延を分析することができます。

CPU Usage

過去 3 分間のリアルタイムの CPU 使用率と最大値が表示されます。

制限：他のレポートを使用してプロセスごとにシステムを監視し、どのプロセスが CPU の問題を引き起こしているのかを判断する必要があります。

Virtual Memory Usage

過去 3 分間のリアルタイム仮想メモリの使用状況および最大値が表示されます。

Common Partition Usage

過去3分間のリアルタイムの共通パーティションの使用率および最大値が表示されます。

Services

サービスの名前、ステータス（サービスが起動しているか、ダウンしているか、管理者によってアクティブ化されたか、停止されたか、開始しているか、停止しているか、または不明な状態か）、およびサーバ、または（該当する場合は）クラスタ内の特定のサーバのサービスが特定の状態にある間に経過した時間を表示します。

Note サービス ステータスが [Unknown State] と表示された場合は、システム サービスの状態を特定できません。

CPU および メモリ

サーバの CPU 使用率、仮想メモリ使用率、メモリ使用率、プロセッサに関する情報を表示します。

CPU Usage

使用された合計 CPU および最後の 3 分間に使用された最大 CPU を表示します。

Virtual Memory Usage

使用された合計仮想メモリおよび最後の 3 分間に使用された最大仮想メモリを表示します。

Memory Usage

次の情報を表示します。

- [% VM Used]：システムのシステム仮想メモリ使用状況のパーセンテージを表します。[% VM Used] カウンタの値は、次の 2 つの式のいずれかから得られる値と等しくなります。

  ```
  (Total KBytes - Free KBytes - Buffers KBytes - Cached KBytes +
  Shared KBytes + Used Swap KBytes ) / (Total KBytes + Total Swap
  KBytes)
  ```

  ```
  Used VM KBytes / Total VM KBytes
  ```

- [Total]：システムのメモリの総量をキロバイト単位で表します。

Used

システムで使用中のシステム物理メモリの容量をキロバイト単位で表します。[Used KBytes] カウンタの値は、次の式から得られる値と等しくなります。

```
Total KBytes - Free KBytes - Buffers KBytes - Cached KBytes + Shared
KBytes
```

[Used KBytes] の値は、top コマンドまたは free コマンド出力で表示される [Linux Used] の値とは異なります。Linux の top コマンドまたは free コマンドの出力に示される used 値は、`Total KBytes - Free KBytes` と等しく、バッファのキロバイト数とキャッシュされたキロバイト数の合計も含んでいます。

Free

システムで使用可能なメモリの総量をキロバイト単位で表します。

Shared

システムの共有メモリの容量をキロバイト単位で表します。

Buffers

システムのバッファの容量をキロバイト単位で表します。

Cached

キャッシュされたメモリの容量をキロバイト単位で表します。

Total Swap

システムのスワップ領域の総量をキロバイト単位で表します。

Used Swap

システムで使用中のスワップ領域の容量をキロバイト単位で表します。

Free Swap

システムで利用可能な空きスワップ領域の容量をキロバイト単位で表します。

Processors

次の情報を表示します。

- [Prosessor]：プロセッサのインスタンス。たとえば、Quad-Core CPU には、0、1、2、3 の 4 基のプロセッサを備えています。

- [%CPU]：最後の更新から経過した、アイドル時間を除くCPU時間のプロセッサの共有。CPU 時間のパーセンテージとして表現されます。
- [User]：CPU がユーザ レベル（アプリケーション）での実行に要した CPU 使用率をパーセンテージで表示します。
- [Nice]：CPU が nice 優先順位のユーザ レベルでの実行に要した CPU 使用率をパーセンテージで表示します。
- [System]：CPU がシステム レベル（カーネル）での実行に要した CPU 使用率をパーセンテージで表示します。
- [Idle]：CPUがアイドル状態にあり、システムに未処理のディスクI/O要求がなかった時間のパーセンテージを表示します。
- [IRQ]：割り込みのためにデバイスに割り当てられた、または処理終了時にコンピュータに信号送信するための割り込み要求の実行にプロセッサが要した時間のパーセンテージを表示します。
- [Soft IRQ]：タスク切り替えを後に遅延させ、パフォーマンスを向上させるためにソフトウェアの割り込み（softirq）の実行にプロセッサが要した時間のパーセンテージを示します。
- [IO Wait]：システムが未処理のディスク I/O 要求がある間に CPU がアイドル状態だった時間のパーセンテージを表示します。

ディスク使用量（Disk Usage）

ノードのディスク使用率に関する情報を表示します。これには、ダッシュレットとして[Common Partition Usage]、[Swap Partition Usage]、[Spare Partition Usage]、[Shared Memory Partition Usage]、[Active Partition Usage]、[Boot Partition Usage] があります。

各ダッシュレットには次の情報が表示されます。

Used

このファイル システムで使用中のディスク領域のパーセンテージを表します。

Max Past 3 min

過去 3 分間のこのファイル システムで使用中のディスク領域をパーセンテージで表します。

Used Space

このファイル システムで使用中のディスク領域の容量をメガバイト単位で表します。

Total Space

このファイルシステムにあるディスク領域全体の容量をメガバイト単位で表します。このカウンタの数値は、システムで確認できるディスク領域のほかの合計サイズ値とは異なる場合があります。これは、[Total Mbytes] カウンタの値が [Used Mbytes] パフォーマンス カウンタと CLI （ステータスを表示）出力で示される [Free] の値の合計であるためです。[Total Mbytes] の値は、予約済みのファイル システムのディスク ブロックの最小空き容量

のパーセンテージを含んでいる [Total] に対するこの CLI 出力未満になります。ファイルシステムが高効率で動作するための十分なディスク領域容量が確保されるよう、最小空き容量を維持します。

プロセス

ノードで実行されているプロセスに関する情報を表示します。

Process

プロセスの名前

PID

タスクの一意のプロセスID。定期的にラッピングされますが、0で再開されることはありません。

& CPU

最後の更新以降に経過した CPU 時間のタスクの共有で、CPU 総時間のパーセンテージで表されます。

Status

タスクのプロセス ステータス：

- 0：実行中です。
- 1：スリープ状態
- 2：無停電ディスクのスリープ
- 3：ゾンビ
- 4：トレースまたは停止（信号）
- 5：ページング
- 6：不明

Shared Memory

タスクが使用している共有メモリのキロバイト（KB）単位の量です。他のプロセスが同じメモリを共有することも可能です。

Nice

タスクのNice値。負のNice値はプロセスの優先順位が高いことを示し、正のNice値はプロセスの優先順位が低いことを表します。Nice値が0の場合、タスクを実行するかどうか判断するときに優先順位を調整しないでください。

VmRSS

コード、データ、およびスタックなどを含む、現在物理メモリ内にある仮想メモリ（Vm）の常駐セット サイズ（RSS）（KB 単位）。

VmSize

タスクが使用している仮想メモリ総量（KB単位）。これには、すべてのコード、データ、共有ライブラリ、およびスワップ アウトされたページが含まれます（仮想イメージ = スワップ サイズ + 常駐サイズ）。

VmData

タスクのヒープの仮想メモリ使用状況（KB 単位）。

Thread Count

現在タスクでグループ化されているスレッドの数。負の値 -1 は、システムのすべてのプロセスおよびスレッドがデフォルトのしきい値を超過したために、スレッド統計情報（Thread オブジェクトのすべてのパフォーマンス カウンタと、Process オブジェクトの Thread Count カウンタを含む）がオフになったため、このカウンタが現在利用できないことを示します。

Datastack Size

タスク メモリ ステータスのスタック サイズ。

Page Fault Count

タスクで発生し、データをメモリにロードすることが必要になったメジャーページフォールトの数を表します。

集約された履歴データ

レポート エンジン情報のレポート履歴実行時間の合計に関する情報を表示します。

Reporting Engine Info Report Historical Runtime Total

レポートの実行にかかった時間の合計（秒）を表示します。

Tomcat

Tomcat は、Tomcat の非セキュアおよびセキュアな Hypertext Transport Protocol（HTTP）コネクタに関する情報を提供します。Tomcat Connector は、要求を受信して応答を送信するエンドポイントを表します。

このコネクタは、Cisco Unified Intelligence Center の Web ページにアクセスするときに発生する HTTP/HTTPS 要求の処理と HTTP/HTTPS 応答の送信を行います。

ここでは、受信した MByte 数、送信した MByte 数、スレッド ビジー、スレッド最大、コネクタ エラー、コネクタ要求に関する情報を表示します。

Cisco Tomcat Connector MBytes Received

Tomcat コネクタが受信したデータの合計数を表示します。

Cisco Tomcat Connector MBytes Sent

Tomcat コネクタが送信したデータの合計数を表示します。

Cisco Tomcat Connector Threads Busy

要求処理スレッドがビジー/使用中である現在の Tomcat コネクタの数を表示します。

Cisco Tomcat Connector Threads Max

要求処理スレッドの Tomcat コネクタの最大数を表示します。

Cisco Tomcat Connector Errors

Tomcat コネクタで発生した HTTP エラー（401 Unauthorized など）の合計数を表示します。

Cisco Tomcat Connector Requests

Tomcat コネクタが処理した要求の合計数を表示します。

ライブ データ

処理されたライブ メッセージ、処理されたライブ メッセージのサイズ、処理中のライブ メッセージの遅延、受信したライブ メッセージのサイズ、受信したライブ メッセージ、および送信したライブ メッセージに関する情報を表示します。

Reporting Engine Info Live Messages Processed

OpenFire に対して処理された Live Data メッセージの合計数を表示します。

Reporting Engine Info Live Messages Processed Size

OpenFire に対して処理中の Live Data メッセージの合計サイズ（バイト）を表示します。

Reporting Engine Info Live Messages Processing Latency

OpenFire に対する Live Data の処理で使用した合計時間（ミリ秒）を表示します。

Reporting Engine Info Live Messages Received Size

ストリーミング データ ソースから受信した Live Data メッセージの合計サイズ（バイト）を表示します。

Reporting Engine Info Live Messages Received

ストリーミング データ ソースから受信した Live Data メッセージの合計数を表示します。

Reporting Engine Info Live Messages Transmitted

ストリーミング データ ソースから送信された Live Data メッセージの合計数を表示します。

Tomcat JVM

Tomcat Java Virtual Machine（JVM）オブジェクトは、Tomcat JVM に関する情報を提供します。これは特に、Unified Intelligence Center が使用する共通リソース メモリのプールを表します。

空きメモリ（KB）、最大メモリ（KB）、および合計メモリ（KB）に関する情報を表示します。

Cisco Tomcat JVM KBytes Memory Free

Tomcat Java Virtual Machine の動的メモリ ブロック（ヒープ メモリ）の空き容量を表示します。動的メモリ ブロックには、Tomcat およびその Web アプリケーションである Unified Intelligence Center などで作成されたすべてのオブジェクトが保存されます。動的メモリの空き容量が少なくなると、追加のメモリが自動的に割り当てられ、（KbytesMemoryTotal カウンタに表示される）合計メモリ サイズが（KbytesMemoryMax カウンタに表示される）

最大容量まで増加します。使用中のメモリ容量は、KbytesMemoryTotal から KBytesMemoryFree の値を減算することで判断できます。

Cisco Tomcat JVM KBytes Memory Max

Unified Intelligence Center Tomcat Java Virtual Machine の動的メモリ ブロックの最大サイズを表示します。

Cisco Tomcat JVM KBytes Memory Total

Tomcat Java Virtual Machine の動的メモリ ブロックの現在の（空きメモリと使用中のメモリを含めた）合計サイズを表示します。

リアルタイム データ

取得されたレポート リアルタイムのセル数、完了したレポート リアルタイム、実行中のレポート リアルタイム、レポート リアルタイムの実行時間、待機中のレポート リアルタイム、および取得されたレポート リアルタイムの行数を表示します。

Reporting Engine Info Report Realtime Cells Retrieved

すべてのデータ ソースから取得されたセルの合計数（行と列の乗算）を表示します。

Reporting Engine Info Report Realtime Completed

正常に実行されたレポートの合計数を表示します。

Reporting Engine Info Report Realtime Running

現在実行中のレポートの数を表示します。Runnable オブジェクトがプールからスレッドを割り当てられている場合、レポートは現在実行中です。これには、使用可能になるまでスレッドの待ち行列で待機しているレポートは含まれません。

Reporting Engine Info Report Realtime Runtime

レポートの実行にかかった時間の合計（秒）を表示します。

Reporting Engine Info Report Realtime Waiting

現在待ち行列で実行を待機しているレポートの合計数を表示します。

Reporting Engine Info Report Realtime Rows Retrieved

Unified Intelligence Center によりデータ ソースから取得された行の合計数を表示します。

リアルタイムの間隔

間隔で取得されたレポート リアルタイムのセル数、間隔で完了したレポート リアルタイム、間隔で実行中のレポート リアルタイム、間隔でのレポート リアルタイムの実行時間、間隔で待機中のレポート リアルタイム、および間隔で取得されたレポート リアルタイムの行数に関する情報を表示します。

Reporting Engine Info Report Realtime Cells Retrieved Interval

直前の間隔ですべてのデータ ソースから取得されたセルの合計数（行と列の乗算）を表示します。

Reporting Engine Info Report Realtime Completed Interval

直前の間隔での完了したカウンタ レポート（H/RT）の変更を表示します。

Reporting Engine Info Report Realtime Running Interval

レポート（H/RT）実行カウンタの間隔測定値を表示します。

Reporting Engine Info Report Realtime Runtime Interval

直前の間隔でのカウンタ レポート（H/RT）ランタイムの変更を表示します。

Reporting Engine Info Report Realtime Waiting Interval

直前の間隔でのカウンタ ReportRealtimeWaiting の変更を表示します。

Reporting Engine Info Report Realtime Rows Retrieved Interval

レポート（H/RT）の RowsRetrievedTotal カウンタの間隔測定値を表示します。

履歴データ

取得されたレポート履歴セル、完了したレポート履歴、取得されたレポート履歴行、実行中のレポート履歴、レポート履歴ランタイム、および待機中のレポート履歴を表示します。

Reporting Engine Info Report Historical Cells Retrieved

すべてのデータ ソースから取得されたセルの合計数（行と列の乗算）を表示します。

Reporting Engine Info Report Historical Completed

正常に実行されたレポートの合計数を表示します。

Reporting Engine Info Report Historical Rows Retrieved

Unified Intelligence Center によりデータ ソースから取得された行の合計数を表示します。

Reporting Engine Info Report Historical Running

現在実行中の（H/RT）レポートの数を表示します。Runnable オブジェクトがプールからスレッドを割り当てられている場合、レポートは現在実行中です。これには、使用可能になるまでスレッドの待ち行列で待機しているレポートは含まれません。

Reporting Engine Info Report Historical Runtime

レポートの実行にかかった時間の合計（秒）を表示します。

Reporting Engine Info Report Historical Waiting

現在待ち行列で実行を待機しているレポートの合計数を表示します。

履歴データの間隔

間隔で取得されたレポート履歴のセル数、間隔で完了したレポート履歴、間隔で取得されたレポート履歴の行数、間隔で実行中のレポート履歴、間隔でのレポート履歴の実行時間、および間隔で待機中のレポート履歴に関する情報を表示します。

Reporting Engine Info Report Historical Cells Retrieved Interval

直前の間隔ですべてのデータ ソースから取得されたセルの合計数（行と列の乗算）を表示します。

Reporting Engine Info Report Historical Completed Interval

直前の間隔での完了したカウンタ レポート（H/RT）の変更を表示します。

Reporting Engine Info Report Historical Rows Retrieved Interval

レポート（H/RT）の RowsRetrievedTotal カウンタの間隔測定値を表示します。

Reporting Engine Info Report Historical Running Interval

レポート（H/RT）実行カウンタの間隔測定値を表示します。

Reporting Engine Info Report Historical Runtime Interval

直前の間隔でのカウンタ レポート（H/RT）ランタイムの変更を表示します。

Reporting Engine Info Report Historical Waiting Interval

直前の間隔でのカウンタ ReportRealtimeWaiting の変更を表示します。

Cisco MediaSense

Cisco Prime Collaboration Assurance には MediaSense ダッシュボードがあります。これはシステムで定義されており、Cisco MediaSense を追加すると使用できます。Cisco Prime Collaboration Assurance では、モニタリングのニーズに基づいてカスタム ダッシュボードを作成することができます。パフォーマンス カウンタの詳細については、『Cisco MediaSense ユーザ ガイド』を参照してください。

ダッシュボードを表示するには、 に移動します。**[モニタ（Monitor）]** > **[システム ビュー（System View）]** > **[パフォーマンス（Performance）]**[クラスタ（Cluster）] ドロップダウン リストから CCE とクラスタを選択し、[ダッシュボード（Dashboard）] ドロップダウン リストから必要なダッシュボードを選択します。選択したダッシュボードに関連する情報が別のダッシュレットに表示されます。各ダッシュレットには、サーバの詳細、現在の使用状況、および直前の 3 分間に受け取った最大値が表示されます。

前提条件：

- Cisco MediaSense は、Cisco Prime Collaboration Assurance で管理する必要があります。
- Cisco MediaSense は、データを Cisco Prime Collaboration Assurance の MediaSense ダッシュボードで表示するには、到達可能にする必要があります。

新しくサポートされる Cisco MediaSense ダッシュボードは次のとおりです。

システムの要約

CPU 使用率、仮想メモリ使用率、共通パーティションの使用率、重要なサービス ステータスに関する情報を表示します。システム管理者は、[システムの概要（System Summary）] ダッシュレットをモニタして、システムの応答の遅延を分析することができます。

CPU Usage

過去 3 分間のリアルタイムの CPU 使用率と最大値が表示されます。

制限：他のレポートを使用してプロセスごとにシステムを監視し、どのプロセスが CPU の問題を引き起こしているのかを判断する必要があります。

Virtual Memory Usage

過去 3 分間のリアルタイム仮想メモリの使用状況および最大値が表示されます。

Common Partition Usage

過去3分間のリアルタイムの共通パーティションの使用率および最大値が表示されます。

Services

サービスの名前、ステータス（サービスが起動しているか、ダウンしているか、管理者によってアクティブ化されたか、停止されたか、開始しているか、停止しているか、または不明な状態か）、およびサーバ、または（該当する場合は）クラスタ内の特定のサーバのサービスが特定の状態にある間に経過した時間を表示します。

Note サービス ステータスが [Unknown State] と表示された場合は、システム サービスの状態を特定できません。

CPU および メモリ

サーバの CPU 使用率、仮想メモリ使用率、メモリ使用率、プロセッサに関する情報を表示します。

CPU Usage

使用された合計 CPU および最後の 3 分間に使用された最大 CPU を表示します。

Virtual Memory Usage

使用された合計仮想メモリおよび最後の 3 分間に使用された最大仮想メモリを表示します。

Memory Usage

次の情報を表示します。

- [% VM Used]：システムのシステム仮想メモリ使用状況のパーセンテージを表します。[% VM Used] カウンタの値は、次の 2 つの式のいずれかから得られる値と等しくなります。

  ```
  (Total KBytes - Free KBytes - Buffers KBytes - Cached KBytes +
  Shared KBytes + Used Swap KBytes ) / (Total KBytes + Total Swap
  KBytes)
  ```

  ```
  Used VM KBytes / Total VM KBytes
  ```

- [Total]：システムのメモリの総量をキロバイト単位で表します。

Used

システムで使用中のシステム物理メモリの容量をキロバイト単位で表します。[Used KBytes] カウンタの値は、次の式から得られる値と等しくなります。

```
Total KBytes - Free KBytes - Buffers KBytes - Cached KBytes + Shared
KBytes
```

[Used KBytes] の値は、top コマンドまたは free コマンド出力で表示される [Linux Used] の値とは異なります。Linux の top コマンドまたは free コマンドの出力に示される used 値は、`Total KBytes - Free KBytes` と等しく、バッファのキロバイト数とキャッシュされたキロバイト数の合計も含んでいます。

Free

システムで使用可能なメモリの総量をキロバイト単位で表します。

Shared

システムの共有メモリの容量をキロバイト単位で表します。

Buffers

システムのバッファの容量をキロバイト単位で表します。

Cached

キャッシュされたメモリの容量をキロバイト単位で表します。

Total Swap

システムのスワップ領域の総量をキロバイト単位で表します。

Used Swap

システムで使用中のスワップ領域の容量をキロバイト単位で表します。

Free Swap

システムで利用可能な空きスワップ領域の容量をキロバイト単位で表します。

Processors

次の情報を表示します。

- [Prosessor]：プロセッサのインスタンス。たとえば、Quad-Core CPU には、0、1、2、3 の 4 基のプロセッサを備えています。
- [% CPU]：最後の更新から経過した、アイドル時間を除く CPU 時間のプロセッサの共有。CPU 時間のパーセンテージとして表現されます。
- [User]：CPU がユーザ レベル（アプリケーション）での実行に要した CPU 使用率をパーセンテージで表示します。
- [Nice]：CPU が nice 優先順位のユーザ レベルでの実行に要した CPU 使用率をパーセンテージで表示します。
- [System]：CPU がシステム レベル（カーネル）での実行に要した CPU 使用率をパーセンテージで表示します。
- [Idle]：CPU がアイドル状態にあり、システムに未処理のディスク I/O 要求がなかった時間のパーセンテージを表示します。
- [IRQ]：割り込みのためにデバイスに割り当てられた、または処理終了時にコンピュータに信号送信するための割り込み要求の実行にプロセッサが要した時間のパーセンテージを表示します。

- [Soft IRQ]：タスク切り替えを後に遅延させ、パフォーマンスを向上させるためにソフトウェアの割り込み（softirq）の実行にプロセッサが要した時間のパーセンテージを示します。
- [IO Wait]：システムが未処理のディスク I/O 要求がある間に CPU がアイドル状態だった時間のパーセンテージを表示します。

ディスク使用量（Disk Usage）

ノードのディスク使用率に関する情報を表示します。これには、ダッシュレットとして[Common Partition Usage]、[Swap Partition Usage]、[Spare Partition Usage]、[Shared Memory Partition Usage]、[Active Partition Usage]、[Boot Partition Usage] があります。

各ダッシュレットには次の情報が表示されます。

Used

このファイル システムで使用中のディスク領域のパーセンテージを表します。

Max Past 3 min

過去 3 分間のこのファイル システムで使用中のディスク領域をパーセンテージで表します。

Used Space

このファイル システムで使用中のディスク領域の容量をメガバイト単位で表します。

Total Space

このファイルシステムにあるディスク領域全体の容量をメガバイト単位で表します。このカウンタの数値は、システムで確認できるディスク領域のほかの合計サイズ値とは異なる場合があります。これは、[Total Mbytes] カウンタの値が [Used Mbytes] パフォーマンス カウンタと CLI （ステータスを表示）出力で示される [Free] の値の合計であるためです。[Total Mbytes] の値は、予約済みのファイル システムのディスク ブロックの最小空き容量のパーセンテージを含んでいる [Total] に対するこの CLI 出力未満になります。ファイルシステムが高効率で動作するための十分なディスク領域容量が確保されるよう、最小空き容量を維持します。

プロセス

ノードで実行されているプロセスに関する情報を表示します。

Process

プロセスの名前

PID

タスクの一意のプロセスID。定期的にラッピングされますが、0で再開されることはありません。

& CPU

最後の更新以降に経過した CPU 時間のタスクの共有で、CPU 総時間のパーセンテージで表されます。

Status

タスクのプロセス ステータス：

- 0：実行中です。
- 1：スリープ状態
- 2：無停電ディスクのスリープ
- 3：ゾンビ
- 4：トレースまたは停止（信号）
- 5：ページング
- 6：不明

Shared Memory

タスクが使用している共有メモリのキロバイト（KB）単位の量です。他のプロセスが同じメモリを共有することも可能です。

Nice

タスクの Nice 値。負の Nice 値はプロセスの優先順位が高いことを示し、正の Nice 値はプロセスの優先順位が低いことを表します。Nice 値が 0 の場合、タスクを実行するかどうか判断するときに優先順位を調整しないでください。

VmRSS

コード、データ、およびスタックなどを含む、現在物理メモリ内にある仮想メモリ（Vm）の常駐セット サイズ（RSS）（KB 単位）。

VmSize

タスクが使用している仮想メモリ総量（KB 単位）。これには、すべてのコード、データ、共有ライブラリ、およびスワップ アウトされたページが含まれます（仮想イメージ = スワップ サイズ + 常駐サイズ）。

VmData

タスクのヒープの仮想メモリ使用状況（KB 単位）。

Thread Count

現在タスクでグループ化されているスレッドの数。負の値 -1 は、システムのすべてのプロセスおよびスレッドがデフォルトのしきい値を超過したために、スレッド統計情報（Thread オブジェクトのすべてのパフォーマンス カウンタと、Process オブジェクトの Thread Count カウンタを含む）がオフになったため、このカウンタが現在利用できないことを示します。

Datastack Size

タスク メモリ ステータスのスタック サイズ。

Page Fault Count

タスクで発生し、データをメモリにロードすることが必要になったメジャーページフォールトの数を表します。

着信コールの分類

録音に分類されるサービス、再生に分類されるサービス、拒否に分類されるサービス、その他に分類されるサービスに関する情報を表示します。

Cisco MediaSense Call Control Service Classified for Recording

録音要求として処理されるコールの数を表示します。

Cisco MediaSense Call Control Service Classified for Playback

再生要求として処理されるコールの数を表示します。

Cisco MediaSense Call Control Service Classified for Reject

設定に基づいて拒否されるコールの数を表示します。

Cisco MediaSense Call Control Service Classified as Anything Else

承認されたけれども再生または録音要求として処理されないコールの数を表示します。

エラー分析

エラーが発生した録音済みセッションのサービス番号、エージェントによる変換要求の拒否、エージェントによる RTSP モニタリング要求の拒否、エージェントによる RTSP 再生要求の拒否、およびエージェントによる未処理ダウンロード要求の拒否に関する情報を表示します。

Cisco MediaSense Call Control Service Number of Recorded Sessions with Errors

録音が完了したが、エラーが発生したセッションの数を表示します。

Cisco MediaSense Storage Management Agent Rejected Convert Requests

拒否された変換要求の数を表示します。

Cisco MediaSense Storage Management Agent Rejected RTSP Monitoring Requests

拒否された RTSP モニタリング要求の数を表示します。

Cisco MediaSense Storage Management Agent Rejected RTSP Playback Requests

拒否された RTSP 再生要求の数を表示します。

Cisco MediaSense Storage Management Agent Rejected Raw Download Requests

拒否された未処理ダウンロード要求の数を表示します。

パフォーマンスの概要

サービスの平均セットアップ遅延、サービスの最大セットアップ遅延、サービスの平均クエリ応答時間、およびサービスの最大クエリ応答時間に関する情報を表示します。

Cisco MediaSense Call Control Service Mean Setup Delay

Unified CM からの SIP Invite の最初の受信と、Unified CM ローリング ウィンドウ時間への SIP 応答との間の平均遅延（ミリ秒単位）を表示します。

Cisco MediaSense Call Control Service Max Setup Delay

Unified CM からの SIP Invite の最初の受信と、Unified CM ローリング ウィンドウ時間への SIP 応答との間の最大遅延（ミリ秒単位）を表示します。

Cisco MediaSense API Service Mean Query Response Time

直前の 1 時間の平均クエリ応答時間を表示します。

Cisco MediaSense API Service Max Query Response Time

直前の 1 時間の最大クエリ応答時間を表示します。

Cisco Unified Contact Center Express

Cisco Prime Collaboration Assurance は、システムが定義し、Unified CCX を追加すると使用可能になる、Cisco Unified Contact Center Express（Unified CCX）ダッシュボードを提供します。Cisco Prime Collaboration Assurance では、モニタリングのニーズに基づいてカスタム ダッシュボードを作成することができます。パフォーマンス カウンタの詳細については、『Unified Contact Center Express 操作ガイド』を参照してください。

ダッシュボードを表示するには、**[モニタ（Monitor）]**> **[システム ビュー（System View）]**> **[パフォーマンス（Performance）]**[Contact Center Express] を選択してドロップダウン リストから[クラスタ（Cluster）]または[デバイス（Device）]を選択し、[ダッシュボード（Dashboard）]のドロップダウン リストから必要なダッシュボードを選択します。選択したダッシュボードに関連する情報が別のダッシュレットに表示されます。各ダッシュレットには、サーバの詳細、現在の使用状況、および直前の 3 分間に受け取った最大値が表示されます。

前提条件：

- Unified CCX は Cisco Prime Collaboration Assurance で管理する必要があります。
- データを Cisco Prime Collaboration Assurance の Contact Center Express ダッシュボードで表示するには、Unified CCX に到達可能である必要があります。

新しくサポートされる Unified CCX ダッシュボードは、次のとおりです。

システムの要約

CPU 使用率、仮想メモリ使用率、共通パーティションの使用率、重要なサービス ステータスに関する情報を表示します。システム管理者は、[システムの概要（System Summary）] ダッシュレットをモニタして、システムの応答の遅延を分析することができます。

CPU Usage

過去 3 分間のリアルタイムの CPU 使用率と最大値が表示されます。

制限：他のレポートを使用してプロセスごとにシステムを監視し、どのプロセスが CPU の問題を引き起こしているのかを判断する必要があります。

Virtual Memory Usage

過去 3 分間のリアルタイム仮想メモリの使用状況および最大値が表示されます。

Common Partition Usage

過去3分間のリアルタイムの共通パーティションの使用率および最大値が表示されます。

Services

サービスの名前、ステータス（サービスが起動しているか、ダウンしているか、管理者によってアクティブ化されたか、停止されたか、開始しているか、停止しているか、または不明な状態か）、およびサーバ、または（該当する場合は）クラスタ内の特定のサーバのサービスが特定の状態にある間に経過した時間を表示します。

Note サービス ステータスが [Unknown State] と表示された場合は、システム サービスの状態を特定できません。

CPU および メモリ

サーバの CPU 使用率、仮想メモリ使用率、メモリ使用率、プロセッサに関する情報を表示します。

CPU Usage

使用された合計 CPU および最後の 3 分間に使用された最大 CPU を表示します。

Virtual Memory Usage

使用された合計仮想メモリおよび最後の 3 分間に使用された最大仮想メモリを表示します。

Memory Usage

次の情報を表示します。

- [% VM Used]：システムのシステム仮想メモリ使用状況のパーセンテージを表します。[% VM Used] カウンタの値は、次の 2 つの式のいずれかから得られる値と等しくなります。

  ```
  (Total KBytes - Free KBytes - Buffers KBytes - Cached KBytes +
  Shared KBytes + Used Swap KBytes ) / (Total KBytes + Total Swap
  KBytes)
  ```

  ```
  Used VM KBytes / Total VM KBytes
  ```

- [Total]：システムのメモリの総量をキロバイト単位で表します。

Used

システムで使用中のシステム物理メモリの容量をキロバイト単位で表します。[Used KBytes] カウンタの値は、次の式から得られる値と等しくなります。

```
Total KBytes - Free KBytes - Buffers KBytes - Cached KBytes + Shared
KBytes
```

[Used KBytes] の値は、top コマンドまたは free コマンド出力で表示される [Linux Used] の値とは異なります。Linux の top コマンドまたは free コマンドの出力に示される used 値は、`Total KBytes - Free KBytes` と等しく、バッファのキロバイト数とキャッシュされたキロバイト数の合計も含んでいます。

Free

システムで使用可能なメモリの総量をキロバイト単位で表します。

Shared

システムの共有メモリの容量をキロバイト単位で表します。

Buffers

システムのバッファの容量をキロバイト単位で表します。

Cached

キャッシュされたメモリの容量をキロバイト単位で表します。

Total Swap

システムのスワップ領域の総量をキロバイト単位で表します。

Used Swap

システムで使用中のスワップ領域の容量をキロバイト単位で表します。

Free Swap

システムで利用可能な空きスワップ領域の容量をキロバイト単位で表します。

Processors

次の情報を表示します。

- [Prosessor]：プロセッサのインスタンス。たとえば、Quad-Core CPU には、0、1、2、3 の 4 基のプロセッサを備えています。
- [% CPU]：最後の更新から経過した、アイドル時間を除く CPU 時間のプロセッサの共有。CPU 時間のパーセンテージとして表現されます。
- [User]：CPU がユーザ レベル（アプリケーション）での実行に要した CPU 使用率をパーセンテージで表示します。
- [Nice]：CPU が nice 優先順位のユーザ レベルでの実行に要した CPU 使用率をパーセンテージで表示します。
- [System]：CPU がシステム レベル（カーネル）での実行に要した CPU 使用率をパーセンテージで表示します。
- [Idle]：CPU がアイドル状態にあり、システムに未処理のディスク I/O 要求がなかった時間のパーセンテージを表示します。
- [IRQ]：割り込みのためにデバイスに割り当てられた、または処理終了時にコンピュータに信号送信するための割り込み要求の実行にプロセッサが要した時間のパーセンテージを表示します。

- [Soft IRQ]：タスク切り替えを後に遅延させ、パフォーマンスを向上させるためにソフトウェアの割り込み（softirq）の実行にプロセッサが要した時間のパーセンテージを示します。
- [IO Wait]：システムが未処理のディスク I/O 要求がある間に CPU がアイドル状態だった時間のパーセンテージを表示します。

ディスク使用量（Disk Usage）

ノードのディスク使用率に関する情報を表示します。これには、ダッシュレットとして[Common Partition Usage]、[Swap Partition Usage]、[Spare Partition Usage]、[Shared Memory Partition Usage]、[Active Partition Usage]、[Boot Partition Usage] があります。

各ダッシュレットには次の情報が表示されます。

Used

このファイル システムで使用中のディスク領域のパーセンテージを表します。

Max Past 3 min

過去 3 分間のこのファイル システムで使用中のディスク領域をパーセンテージで表します。

Used Space

このファイル システムで使用中のディスク領域の容量をメガバイト単位で表します。

Total Space

このファイルシステムにあるディスク領域全体の容量をメガバイト単位で表します。このカウンタの数値は、システムで確認できるディスク領域のほかの合計サイズ値とは異なる場合があります。これは、[Total Mbytes] カウンタの値が [Used Mbytes] パフォーマンス カウンタと CLI （ステータスを表示）出力で示される [Free] の値の合計であるためです。[Total Mbytes] の値は、予約済みのファイル システムのディスク ブロックの最小空き容量のパーセンテージを含んでいる [Total] に対するこの CLI 出力未満になります。ファイルシステムが高効率で動作するための十分なディスク領域容量が確保されるよう、最小空き容量を維持します。

プロセス

ノードで実行されているプロセスに関する情報を表示します。

Process

プロセスの名前

PID

タスクの一意のプロセスID。定期的にラッピングされますが、0で再開されることはありません。

& CPU

最後の更新以降に経過した CPU 時間のタスクの共有で、CPU 総時間のパーセンテージで表されます。

Status

タスクのプロセス ステータス：

- 0：実行中です。
- 1：スリープ状態
- 2：無停電ディスクのスリープ
- 3：ゾンビ
- 4：トレースまたは停止（信号）
- 5：ページング
- 6：不明

Shared Memory

タスクが使用している共有メモリのキロバイト（KB）単位の量です。他のプロセスが同じメモリを共有することも可能です。

Nice

タスクの Nice 値。負の Nice 値はプロセスの優先順位が高いことを示し、正の Nice 値はプロセスの優先順位が低いことを表します。Nice 値が 0 の場合、タスクを実行するかどうか判断するときに優先順位を調整しないでください。

VmRSS

コード、データ、およびスタックなどを含む、現在物理メモリ内にある仮想メモリ（Vm）の常駐セット サイズ（RSS）（KB 単位）。

VmSize

タスクが使用している仮想メモリ総量（KB 単位）。これには、すべてのコード、データ、共有ライブラリ、およびスワップ アウトされたページが含まれます（仮想イメージ = スワップ サイズ + 常駐サイズ）。

VmData

タスクのヒープの仮想メモリ使用状況（KB 単位）。

Thread Count

現在タスクでグループ化されているスレッドの数。負の値 -1 は、システムのすべてのプロセスおよびスレッドがデフォルトのしきい値を超過したために、スレッド統計情報（Thread オブジェクトのすべてのパフォーマンス カウンタと、Process オブジェクトの Thread Count カウンタを含む）がオフになったため、このカウンタが現在利用できないことを示します。

Datastack Size

タスク メモリ ステータスのスタック サイズ。

Page Fault Count

タスクで発生し、データをメモリにロードすることが必要になったメジャーページフォールトの数を表します。

Virtualized Voice Browser

Cisco Prime Collaboration Assurance は、システムが定義し、Virtualized Voice Browser を追加すると利用可能になる、Virtualized Voice Browser ダッシュボードを提供します。Cisco Prime Collaboration Assurance では、モニタリングのニーズに基づいてカスタム ダッシュボードを作成することができます。

ダッシュボードを表示するには、**[モニタ（Monitor）]** > **[システム ビュー（System View）]** > **[パフォーマンス（Performance）]**で、[クラスタ（Cluster or Device）ドロップダウン リストから [仮想化音声ブラウザ（Virtualized Voice Browser）とデバイスの IP アドレス/ホスト名] を選択し、[ダッシュボード（Dashboard] ドロップダウン リストから必要なダッシュボードを選択します。選択したダッシュボードに関連する情報が別のダッシュレットに表示されます。各ダッシュレットには、サーバの詳細、現在の使用状況、および直前の3分間に受け取った最大値が表示されます。

前提条件：

- Virtualized Voice Browser は、Cisco Prime Collaboration Assurance で管理する必要があります。
- データを Cisco Prime Collaboration Assurance の Virtualized Voice Browser ダッシュボードで表示するには、Virtualized Voice Browser に到達可能である必要があります。

新しくサポートされる Virtualized Voice Browser ダッシュボードは、次のとおりです。

システムの要約

CPU 使用率、仮想メモリ使用率、共通パーティションの使用率、重要なサービス ステータスに関する情報を表示します。システム管理者は、[システムの概要（System Summary）] ダッシュレットをモニタして、システムの応答の遅延を分析することができます。

CPU Usage

過去 3 分間のリアルタイムの CPU 使用率と最大値が表示されます。

制限：他のレポートを使用してプロセスごとにシステムを監視し、どのプロセスが CPU の問題を引き起こしているのかを判断する必要があります。

Virtual Memory Usage

過去 3 分間のリアルタイム仮想メモリの使用状況および最大値が表示されます。

Common Partition Usage

過去3分間のリアルタイムの共通パーティションの使用率および最大値が表示されます。

Services

サービスの名前、ステータス（サービスが起動しているか、ダウンしているか、管理者によってアクティブ化されたか、停止されたか、開始しているか、停止しているか、または

不明な状態か）、およびサーバ、または（該当する場合は）クラスタ内の特定のサーバのサービスが特定の状態にある間に経過した時間を表示します。

Note サービス ステータスが [Unknown State] と表示された場合は、システム サービスの状態を特定できません。

CPU および メモリ

サーバの CPU 使用率、仮想メモリ使用率、メモリ使用率、プロセッサに関する情報を表示します。

CPU Usage

使用された合計 CPU および最後の 3 分間に使用された最大 CPU を表示します。

Virtual Memory Usage

使用された合計仮想メモリおよび最後の 3 分間に使用された最大仮想メモリを表示します。

Memory Usage

次の情報を表示します。

- [% VM Used]：システムのシステム仮想メモリ使用状況のパーセンテージを表します。[% VM Used] カウンタの値は、次の 2 つの式のいずれかから得られる値と等しくなります。

  ```
  (Total KBytes - Free KBytes - Buffers KBytes - Cached KBytes + Shared KBytes + Used Swap KBytes ) / (Total KBytes + Total Swap KBytes)
  ```

  ```
  Used VM KBytes / Total VM KBytes
  ```

- [Total]：システムのメモリの総量をキロバイト単位で表します。

Used

システムで使用中のシステム物理メモリの容量をキロバイト単位で表します。[Used KBytes] カウンタの値は、次の式から得られる値と等しくなります。

```
Total KBytes - Free KBytes - Buffers KBytes - Cached KBytes + Shared KBytes
```

[Used KBytes] の値は、top コマンドまたは free コマンド出力で表示される [Linux Used] の値とは異なります。Linux の top コマンドまたは free コマンドの出力に示される used 値は、`Total KBytes - Free KBytes` と等しく、バッファのキロバイト数とキャッシュされたキロバイト数の合計も含んでいます。

Free

システムで使用可能なメモリの総量をキロバイト単位で表します。

Shared

システムの共有メモリの容量をキロバイト単位で表します。

Buffers

システムのバッファの容量をキロバイト単位で表します。

Cached

キャッシュされたメモリの容量をキロバイト単位で表します。

Total Swap

システムのスワップ領域の総量をキロバイト単位で表します。

Used Swap

システムで使用中のスワップ領域の容量をキロバイト単位で表します。

Free Swap

システムで利用可能な空きスワップ領域の容量をキロバイト単位で表します。

Processors

次の情報を表示します。

- [Prosessor]：プロセッサのインスタンス。たとえば、Quad-Core CPU には、0、1、2、3 の 4 基のプロセッサを備えています。
- [% CPU]：最後の更新から経過した、アイドル時間を除く CPU 時間のプロセッサの共有。CPU 時間のパーセンテージとして表現されます。
- [User]：CPU がユーザ レベル（アプリケーション）での実行に要した CPU 使用率をパーセンテージで表示します。
- [Nice]：CPU が nice 優先順位のユーザ レベルでの実行に要した CPU 使用率をパーセンテージで表示します。
- [System]：CPU がシステム レベル（カーネル）での実行に要した CPU 使用率をパーセンテージで表示します。
- [Idle]：CPU がアイドル状態にあり、システムに未処理のディスク I/O 要求がなかった時間のパーセンテージを表示します。
- [IRQ]：割り込みのためにデバイスに割り当てられた、または処理終了時にコンピュータに信号送信するための割り込み要求の実行にプロセッサが要した時間のパーセンテージを表示します。
- [Soft IRQ]：タスク切り替えを後に遅延させ、パフォーマンスを向上させるためにソフトウェアの割り込み（softirq）の実行にプロセッサが要した時間のパーセンテージを示します。
- [IO Wait]：システムが未処理のディスク I/O 要求がある間に CPU がアイドル状態だった時間のパーセンテージを表示します。

ディスク使用量（Disk Usage）

ノードのディスク使用率に関する情報を表示します。これには、ダッシュレットとして[Common Partition Usage]、[Swap Partition Usage]、[Spare Partition Usage]、[Shared Memory Partition Usage]、[Active Partition Usage]、[Boot Partition Usage] があります。

各ダッシュレットには次の情報が表示されます。

Used

このファイル システムで使用中のディスク領域のパーセンテージを表します。

Max Past 3 min

過去 3 分間のこのファイル システムで使用中のディスク領域をパーセンテージで表します。

Used Space

このファイル システムで使用中のディスク領域の容量をメガバイト単位で表します。

Total Space

このファイルシステムにあるディスク領域全体の容量をメガバイト単位で表します。このカウンタの数値は、システムで確認できるディスク領域のほかの合計サイズ値とは異なる場合があります。これは、[Total Mbytes] カウンタの値が [Used Mbytes] パフォーマンス カウンタと CLI （ステータスを表示）出力で示される [Free] の値の合計であるためです。[Total Mbytes] の値は、予約済みのファイル システムのディスク ブロックの最小空き容量のパーセンテージを含んでいる [Total] に対するこの CLI 出力未満になります。ファイル システムが高効率で動作するための十分なディスク領域容量が確保されるよう、最小空き容量を維持します。

プロセス

ノードで実行されているプロセスに関する情報を表示します。

Process

プロセスの名前

PID

タスクの一意のプロセスID。定期的にラッピングされますが、0で再開されることはありません。

& CPU

最後の更新以降に経過した CPU 時間のタスクの共有で、CPU 総時間のパーセンテージで表されます。

Status

タスクのプロセス ステータス：

- 0：実行中です。
- 1：スリープ状態

- 2：無停電ディスクのスリープ
- 3：ゾンビ
- 4：トレースまたは停止（信号）
- 5：ページング
- 6：不明

Shared Memory

タスクが使用している共有メモリのキロバイト（KB）単位の量です。他のプロセスが同じメモリを共有することも可能です。

Nice

タスクの Nice 値。負の Nice 値はプロセスの優先順位が高いことを示し、正の Nice 値はプロセスの優先順位が低いことを表します。Nice 値が 0 の場合、タスクを実行するかどうか判断するときに優先順位を調整しないでください。

VmRSS

コード、データ、およびスタックなどを含む、現在物理メモリ内にある仮想メモリ（Vm）の常駐セット サイズ（RSS）（KB 単位）。

VmSize

タスクが使用している仮想メモリ総量（KB 単位）。これには、すべてのコード、データ、共有ライブラリ、およびスワップ アウトされたページが含まれます（仮想イメージ = スワップ サイズ + 常駐サイズ）。

VmData

タスクのヒープの仮想メモリ使用状況（KB 単位）。

Thread Count

現在タスクでグループ化されているスレッドの数。負の値 -1 は、システムのすべてのプロセスおよびスレッドがデフォルトのしきい値を超過したために、スレッド統計情報（Thread オブジェクトのすべてのパフォーマンス カウンタと、Process オブジェクトの Thread Count カウンタを含む）がオフになったため、このカウンタが現在利用できないことを示します。

Datastack Size

タスク メモリ ステータスのスタック サイズ。

Page Fault Count

タスクで発生し、データをメモリにロードすることが必要になったメジャーページフォールトの数を表します。

パフォーマンス ダッシュボード

[パフォーマンス（Performance）] ページには、パフォーマンス カウンタに基づいたシステム定義のダッシュボードが表示されます。

（注）

- Unified Communications Manager でクラスタ名とホスト名の両方が同じである場合に、選択したクラスタのパフォーマンス ダッシュボードを表示するには、クラスタ名前を変更し、Cisco Prime Collaboration Assurance で Unified Communications Manager を再検出する必要があります。
- パフォーマンス カウンタ 用のカスタム ダッシュボードを作成済みの場合は、次のデバイス タイプのために、Cisco Prime Collaboration Assurance 12.1 でも同じように再設定する必要があります。

[デバイス タイプ（Device Type）]	**[バージョン（Version）]**
Finesse	[10 以上（10 or higher）]
Socialminer	[10 以上（10 or higher）]

ダッシュボードを表示するには、[Cluster] または [Device] ドロップダウン リストから製品とクラスタを選択し、[Dashboard] ドロップダウン リストから必要なダッシュボードを選択します。

すべてのクラスタまたはデバイスについてのシステム定義のダッシュボードに加えて、トレンドダッシュボードを使用して、デバイス関連のメトリックのトレンドを表示することもできます。トレンドを表示される方法の詳細については、[Trend] ダッシュボードを参照してください。

Cisco Prime Collaboration リリース 11.1 以降の場合

Unified CM と Unity Connection

Unified CM では、次のシステム定義のダッシュボードを使用できます。

（注） Unity Connection では、[System Summary]、[CPU and Memory]、[Disk Usage]、[Process]、[Port Monitor] というダッシュレットのみが表示されます。

システムの要約

CPU 使用率、仮想メモリ使用率、共通パーティションの使用率、重要なサービス ステータスに関する情報を表示します。システム管理者は、[システムの概要（System Summary）] ダッシュレットをモニタして、システムの応答の遅延を分析することができます。

CPU Usage

過去 3 分間のリアルタイムの CPU 使用率と最大値が表示されます。

制限：他のレポートを使用してプロセスごとにシステムを監視し、どのプロセスが CPU の問題を引き起こしているのかを判断する必要があります。

Virtual Memory Usage

過去 3 分間のリアルタイム仮想メモリの使用状況および最大値が表示されます。

Common Partition Usage

過去3分間のリアルタイムの共通パーティションの使用率および最大値が表示されます。

Services

サービスの名前、ステータス（サービスが起動しているか、ダウンしているか、管理者によってアクティブ化されたか、停止されたか、開始しているか、停止しているか、または不明な状態か）、およびサーバ、または（該当する場合は）クラスタ内の特定のサーバのサービスが特定の状態にある間に経過した時間を表示します。

Note サービス ステータスが [Unknown State] と表示された場合は、システム サービスの状態を特定できません。

Communications Manager の概要

登録済みの電話機、進行中のコール、およびアクティブなゲートウェイ ポートとチャネルを表示します。

Registered Phones

登録済みの電話機の総数、および直前に登録された電話機数の差分を表示します。負の値は電話機が登録解除されたことを示し、正の値は新しい電話機が登録されたことを示します。

Calls in Progress

進行中のコールの総数と、直前の進行中の差分コール数を表示します。負の値は、コールが完了した、またはドロップされたことを示し、正の値は新しいコールが確立されたことを示します。

Active MGCP Ports and Channels

アクティブな MGCP ポートとチャネルの総数と、過去数分のアクティブな MGCP ポートとチャネルの差分を表示します。負の値はアクティブな MGCP ポートとチャネルが減少したことを示し、正の値はアクティブな MGCP ポートとチャネルが増加したことを示します。

Call Activity

Call Activity

Cisco Unified Communications Manager の、完了したコール、試行されたコール、進行中のコール、論理パーティション合計エラー数などのコールアクティビティを表示します。該当する場合、これはクラスタ内のすべてのサーバが含まれます。

Calls Completed

Cisco Unified Communications Manager を使用して、実際に接続された（音声パスまたはビデオストリームが確立された）コールの数を表示します。この数は、コールが終了したときに増加します。

Calls Attempted

試行されたコールの合計数を表示します。試行されたコールは、どの番号がダイヤルされたか、または宛先に接続されたかに関係なく、電話機がオフフックになるとき、およびオンフックに戻るときに必ず発生します。機能操作（たとえば、転送や会議）中のコールの試行も、試行されたコールと見なされます。

Calls in Progress

進行中のコールと過去1分間に進行中だった差分コールの総数を表示します。負の値は、コールが完了またはドロップされたことを示し、正の値は新しいコールが確立されたことを示します。

Logical Partition Failures

論理パーティションエラーの総数を表示します。また、過去1分間の論理パーティションエラーの差分を表示します。

ゲートウェイ アクティビティ

アクティブポート、サービス中のポート、完了したコールを含むCisco Unified Communications Managerのゲートウェイアクティビティを表示します。ゲートウェイのアクティビティには、該当する場合は、クラスタのすべてのノードが含まれます。

MGCP FXS

- Ports in Service：システムで現在使用可能な FXS ポートの数を表示します。
- Ports Active：この Unified CM で現在使用中の（アクティブな）FXS ポートの数を表示します。
- Calls Completed：MGCP FXS デバイス上のすべての FXS ポート インスタンスから発信され成功したコールの総数を表示します。

MGCP FXO

- Ports in Service：システムで現在使用可能な FXO ポートの数を表示します。
- Ports Active：この Unified CM で現在使用中の（アクティブな）FXO ポートの数を表示します。

- Calls Completed：MGCP FXO デバイス上のすべての FXO ポート インスタンスから発信され、成功したコールの総数を表示します。

MGCP T1

- Spans in Service：現在使用可能な T1 CAS スパンの数を表示します。
- Channel Active：この Unified CM 上でアクティブ コールにある T1 CAS 音声チャネルが表示されます。
- Calls Completed：MGCP T1 CAS デバイスのすべてのインスタンスから発信され、成功したコールの総数を表示します。

MGCP PRI

- Spans In Service：現在使用可能な PRI スパンの数を表示します。
- Channel Active：この Unified CM のアクティブ コールにある PRI 音声チャネルの数を表します。
- Calls Completed：MGCP PRI デバイスのすべてのインスタンスからの発信され、成功したコールの総数を表示します。

進行中のコールおよび完了したコールを含む Cisco Unified Communications Manager 上のトランク アクティビティを表示します。このカウンタには、該当する場合は、クラスタ内のすべてのノードが含まれます。

H323

Calls In Progress：Cisco H323 デバイスのすべてのインスタンスで現在進行中のコールの総数を表示します。

Calls Completed：Cisco H323 デバイスのすべてのインスタンスから発信され、成功したコールの総数を表示します。

SIP Trunk

Calls In Progress：アクティブなすべてのコールを含め、SIP デバイスのすべてのインスタンスで現在進行中のコールの総数を表示します。進行中のすべてのコールが接続されると、進行中のコールの数とアクティブなコールの数は同じになります。

Calls In Progress：SIP デバイスのすべてのインスタンスから実際に接続された（音声パスが確立された）コールの総数を表示します。この数は、コールが終了すると増分します。

SDL キュー

キューに格納されている信号の数や処理済みの信号の数などの SDL キュー情報が表示されます。

Signals in SDL Queue

[High]：Unified CM キューの高優先順位信号の数を表します。高優先順位信号には、主に、タイムアウト イベント、内部 Unified Communications Manager キープアライブ、特定のゲートキーパーイベント、内部プロセスの作成などのイベントが含まれています。多数

の高優先順位イベントは、Unified CM のパフォーマンスを低下させ、コール接続の遅延やダイヤル トーン消失の原因となります。このカウンタを Queue Signals Processed High カウンタと併用して、Unified CM 上の処理の遅延を判別します。

[Normal]：Unified CM キューの通常優先順位信号の数を表します。通常優先順位信号には、主に、コール処理機能、キー操作、オンフックとオフフックの通知などのイベントが含まれています。多数の通常優先順位のイベントは、Unified CM のパフォーマンスを低下させ、ダイヤル トーンの遅延、コール接続の遅延、またはダイヤル トーンの消失の原因となる場合があります。このカウンタを Queue Signals Processed Normal カウンタと併用して、Unified CM 上のコール処理の遅延を判別します。通常優先順位信号が処理を開始する前に、高優先順位信号を完了する必要があることに注意してください。したがって、高優先順位カウンタを確認し、遅延の可能性について正確な状況を把握する必要があります。

[Low]：Unified CM キューの低優先順位信号の数を表します。低優先順位信号には、主に、端末デバイスの登録（初期端末登録要求メッセージは除く）などのイベントが含まれています。このキュー内の多数の信号は、デバイス登録遅延の原因となります。

[Lowest]：Unified CM キューの最低優先順位信号の数を表します。最低優先順位信号には、デバイス登録中の初期端末登録要求メッセージが含まれています。このキュー内の多数の信号は、デバイス登録遅延の原因となります。

Processed SDL Signals

[High]：1 秒間隔で Unified CM により処理される高優先順位信号の数を表します。このカウンタを Queue Signals Present High カウンタと併用して、このキューの処理の遅延を判別します。

[Normal]：1 秒間隔で Unified CM により処理される通常優先順位信号の数を表します。このカウンタを Queue Signals Present Normal カウンタと併用して、このキューの処理の遅延を判別します。高優先順位信号は通常優先順位信号の前に処理されることに注意してください。

[Low]：1 秒間隔で Unified CM により処理される低優先順位信号の数を表します。このカウンタを Queue Signals Present Low カウンタと併用して、このキューの処理の遅延を判別します。処理される信号の数は、この時間間隔でデバイス登録アクティビティが処理される量の指標となります。

[Lowest]：1 秒間隔で Unified CM により処理される最低優先順位信号の数を表します。このカウンタを Queue Signals Present Lowest カウンタと併用して、このキューの処理の遅延を判別します。処理される信号の数は、この時間間隔で Unified CM 登録プロセスを開始したデバイスの数の指標となります。

Cisco TFTP

合計 TFTP 要求数、見つかった合計 TFTP 要求数、および異常終了した合計 TFTP 要求数を含めて、Cisco Unified Communications Manager ノードの Cisco Trivial File Transfer Protocol（TFTP）のステータスを表示します。

TFTP Requests

該当する場合、このカウンタにはクラスタ内のすべてのノードが含まれます。このカウンタは、TFTP サーバが処理するファイル要求（XML 設定ファイル、電話機ファームウェア

ファイル、オーディオファイルに対する要求）の総数を表します。このカウンタは、TFTP サービス開始後の RequestsProcessed、RequestsNotFound、RequestsOverflow、RequestsAborted、RequestsInProgress の各カウンタを合計した数になります。

CPU および メモリ

サーバの CPU 使用率、仮想メモリ使用率、メモリ使用率、プロセッサに関する情報を表示します。

CPU Usage

使用された合計 CPU および最後の 3 分間に使用された最大 CPU を表示します。

Virtual Memory Usage

使用された合計仮想メモリおよび最後の 3 分間に使用された最大仮想メモリを表示します。

Memory Usage

次の情報を表示します。

- [% VM Used]：システムのシステム仮想メモリ使用状況のパーセンテージを表します。[% VM Used] カウンタの値は、次の 2 つの式のいずれかから得られる値と等しくなります。

  ```
  (Total KBytes - Free KBytes - Buffers KBytes - Cached KBytes +
  Shared KBytes + Used Swap KBytes ) / (Total KBytes + Total Swap
  KBytes)
  ```

  ```
  Used VM KBytes / Total VM KBytes
  ```

- [Total]：システムのメモリの総量をキロバイト単位で表します。

Used

システムで使用中のシステム物理メモリの容量をキロバイト単位で表します。[Used KBytes] カウンタの値は、次の式から得られる値と等しくなります。

```
Total KBytes - Free KBytes - Buffers KBytes - Cached KBytes + Shared
KBytes
```

[Used KBytes] の値は、top コマンドまたは free コマンド出力で表示される [Linux Used] の値とは異なります。Linux の top コマンドまたは free コマンドの出力に示される used 値は、`Total KBytes - Free KBytes` と等しく、バッファのキロバイト数とキャッシュされたキロバイト数の合計も含んでいます。

Free

システムで使用可能なメモリの総量をキロバイト単位で表します。

Shared

システムの共有メモリの容量をキロバイト単位で表します。

Buffers

システムのバッファの容量をキロバイト単位で表します。

Cached

キャッシュされたメモリの容量をキロバイト単位で表します。

Total Swap

システムのスワップ領域の総量をキロバイト単位で表します。

Used Swap

システムで使用中のスワップ領域の容量をキロバイト単位で表します。

Free Swap

システムで利用可能な空きスワップ領域の容量をキロバイト単位で表します。

Processors

次の情報を表示します。

- [Prosessor]：プロセッサのインスタンス。たとえば、Quad-Core CPU には、0、1、2、3 の 4 基のプロセッサを備えています。
- [% CPU]：最後の更新から経過した、アイドル時間を除く CPU 時間のプロセッサの共有。CPU 時間のパーセンテージとして表現されます。
- [User]：CPU がユーザ レベル（アプリケーション）での実行に要した CPU 使用率をパーセンテージで表示します。
- [Nice]：CPU が nice 優先順位のユーザ レベルでの実行に要した CPU 使用率をパーセンテージで表示します。
- [System]：CPU がシステム レベル（カーネル）での実行に要した CPU 使用率をパーセンテージで表示します。
- [Idle]：CPU がアイドル状態にあり、システムに未処理のディスク I/O 要求がなかった時間のパーセンテージを表示します。
- [IRQ]：割り込みのためにデバイスに割り当てられた、または処理終了時にコンピュータに信号送信するための割り込み要求の実行にプロセッサが要した時間のパーセンテージを表示します。
- [Soft IRQ]：タスク切り替えを後に遅延させ、パフォーマンスを向上させるためにソフトウェアの割り込み（softirq）の実行にプロセッサが要した時間のパーセンテージを示します。
- [IO Wait]：システムが未処理のディスク I/O 要求がある間に CPU がアイドル状態だった時間のパーセンテージを表示します。

ディスク使用量（Disk Usage）

ノードのディスク使用率に関する情報を表示します。これには、ダッシュレットとして [Common Partition Usage]、[Swap Partition Usage]、[Spare Partition Usage]、[Shared Memory Partition Usage]、[Active Partition Usage]、[Boot Partition Usage] があります。

各ダッシュレットには次の情報が表示されます。

Used

このファイル システムで使用中のディスク領域のパーセンテージを表します。

Max Past 3 min

過去 3 分間のこのファイル システムで使用中のディスク領域をパーセンテージで表します。

Used Space

このファイル システムで使用中のディスク領域の容量をメガバイト単位で表します。

Total Space

このファイルシステムにあるディスク領域全体の容量をメガバイト単位で表します。このカウンタの数値は、システムで確認できるディスク領域のほかの合計サイズ値とは異なる場合があります。これは、[Total Mbytes] カウンタの値が [Used Mbytes] パフォーマンス カウンタと CLI （ステータスを表示）出力で示される [Free] の値の合計であるためです。[Total Mbytes] の値は、予約済みのファイル システムのディスク ブロックの最小空き容量のパーセンテージを含んでいる [Total] に対するこの CLI 出力未満になります。ファイル システムが高効率で動作するための十分なディスク領域容量が確保されるよう、最小空き容量を維持します。

CTI Manager

CTI Manager とインターフェイスするデバイスおよびアプリケーションに関する情報を表示します。次の情報が表示されます。

Open Devices

CTI Manager に接続されたすべてのアプリケーションによって開かれたデバイスの数。

Open Lines

CTI Manager に接続されたすべてのアプリケーションによって開かれた回線の数。

CTI Connection

CTI Manager に接続されたアプリケーションの数。

CM Links

CTI Manager へのアクティブな Unified Communication Manager リンク。

ハートビート

Cisco Unified Communications Manager と Cisco TFTP サービスの表示ハートビート情報を表示します。

CMs Heartbeat

[Current Value] は、Unified CM のハートビートを表します。これは、Unified CM が実行していることを示す増分カウントです。カウンタが増加していない場合は、Unified CM がダウンしています。1 分を超えるとデルタが表示されます。値 0 は Unified Communications Manager ダウンしていることを示します。

TFTPs Heartbeat

現在の値は TFTP サーバのハートビートを表します。これは、TFTP サーバが動作していることを示す増分カウントです。カウンタが増加していない場合は、TFTP サーバがダウンしています。1 分を超えるとデルタが表示されます。値 0 は、TFTP サーバがダウンしていることを示します。

SIP アクティビティ

Cisco Unified Communications Manager 上の概要要求、概要応答、着信失敗応答の概要、発信失敗応答の概要、発信再試行要求、発信再試行応答などの SIP アクティビティを表示します。該当する場合、SIP アクティビティにはクラスタ内のすべてのノードが含まれます。

Summary Requests

再転送数 + デバイスが送信（発信およびリレー）した SIP 要求メッセージの総数などを含め、SIP デバイスが受信した SIP 要求メッセージの総数の要約が表示されます。特定のメッセージが複数回送信された場合（たとえば、再転送または結果のフォーク）、各転送は別々にカウントされます。

Summary Responses

再転送 + SIP デバイスが送信（発信およびリレー）した SIP 応答メッセージの総数（再転送を含む）などを含め、SIP デバイスが受信した SIP 応答メッセージの総数の要約が表示されます。

Summary Failure Responses In

SIP デバイスが受信した、4xx クラスの SIP 応答の総数（転送数を含む）が表示されます。このクラスの応答は、クライアント機能を提供する SIP デバイスによる要求失敗 + SIP デバイスが受信した 5xx クラスの SIP 応答の総数（転送を含む）を示します。このクラスの応答は、クライアント機能を提供する SIP デバイスが受信した失敗応答 + SIP デバイスが受信した 6xx クラスの SIP 応答の総数（転送を含む）を示します。このクラスの応答は、クライアント機能を提供する SIP デバイスが受信した失敗応答を示します。応答は一般に、Request-URI で示された特定のインスタンスだけでなく、ノードが特定の着信側に関して明確な情報を持つことを示します。

Summary Failure Responses Out

SIP デバイスが送信した、4xx クラスの SIP 応答の総数（転送数を含む）が表示されます。このクラスの応答は、ノード機能を提供する SIP デバイスによる要求失敗 + SIP デバイスが送信した 5xx クラスの SIP 応答の総数（転送を含む）を示します。このクラスの応答は、ノード機能を提供する SIP デバイスが送信した失敗応答 + SIP デバイスが送信した 6xx クラスの SIP 応答の総数（転送を含む）を示します。このクラスの応答は、ノード機能を提供する SIP デバイスが送信した失敗応答を示します。応答は一般に、Request-URI で示された特定のインスタンスだけでなく、ノードが特定の着信側に関して明確な情報を持つことを示します。

Retry Requests Out

SIP デバイスが送信した要求再試行の合計回数を表示します。

Retry Responses Out

SIP デバイスが送信した最終応答再試行の総回数 + SIP デバイスが送信した最終以外の応答再試行の総回数の要約を表示します。

プロセス

ノードで実行されているプロセスに関する情報を表示します。

Process

プロセスの名前

PID

タスクの一意のプロセスID。定期的にラッピングされますが、0で再開されることはありません。

& CPU

最後の更新以降に経過した CPU 時間のタスクの共有で、CPU 総時間のパーセンテージで表されます。

Status

タスクのプロセス ステータス：

- 0：実行中です。
- 1：スリープ状態
- 2：無停電ディスクのスリープ
- 3：ゾンビ
- 4：トレースまたは停止（信号）
- 5：ページング
- 6：不明

Shared Memory

タスクが使用している共有メモリのキロバイト（KB）単位の量です。他のプロセスが同じメモリを共有することも可能です。

Nice

タスクの Nice 値。負の Nice 値はプロセスの優先順位が高いことを示し、正の Nice 値はプロセスの優先順位が低いことを表します。Nice値が0の場合、タスクを実行するかどうか判断するときに優先順位を調整しないでください。

VmRSS

コード、データ、およびスタックなどを含む、現在物理メモリ内にある仮想メモリ（Vm）の常駐セット サイズ（RSS）（KB 単位）。

VmSize

タスクが使用している仮想メモリ総量（KB単位）。これには、すべてのコード、データ、共有ライブラリ、およびスワップ アウトされたページが含まれます（仮想イメージ = スワップ サイズ + 常駐サイズ）。

VmData

タスクのヒープの仮想メモリ使用状況（KB 単位）。

Thread Count

現在タスクでグループ化されているスレッドの数。負の値 -1 は、システムのすべてのプロセスおよびスレッドがデフォルトのしきい値を超過したために、スレッド統計情報（Thread オブジェクトのすべてのパフォーマンス カウンタと、Process オブジェクトの Thread Count カウンタを含む）がオフになったため、このカウンタが現在利用できないことを示します。

Datastack Size

タスク メモリ ステータスのスタック サイズ。

Page Fault Count

タスクで発生し、データをメモリにロードすることが必要になったメジャーページフォールトの数を表します。

データベースの概要

サーバの接続情報を提供します。データベースのキューに格納されている変更通知要求、メモリのキューに格納されている変更通知要求、アクティブなクライアント接続の総数、デバイスリセットのためにキューに格納されているデバイス数、作成された複製の数、複製のステータスなどの情報です。

Change Notification Requests Queued in DB

DBCNQueue テーブルのレコード数を表示します。

Change Notification Requests Queued in Memory

メモリのキューに格納される変更通知要求の数を表示します。

Total Number of Connection Clients

メモリのキューに格納される変更通知要求の数を表示します。

Replicates Created

Informix によって DB テーブル用に作成された複製の数を表示します。すべてのテーブルに、少なくとも 1 個の複製が含まれます。このカウンタは、複製のセットアップ中の情報を表示します。

Replication Status

複製の状態を表示します。

- 0 = ReplTask スレッド初期化中
- 1 = このノードから開始された複製セットアップ スクリプト

- 2 : 複製が有効です。複製が正しく設定され、データベース内のほとんどのテーブルがクラスタのすべてのノードで同期されている必要があります。

Note Rすべてのテーブルが同期していることを確認するには、CLI コマンド **utils dbreplication status**を実行します

- 3 = クラスタ内での複製データの転送に問題があります。

Note カウンタに表示された値が 3 である場合は、クラスタでの複製に問題があります。この値は、複製がその特定のノードで問題であるという意味ではありません。CLI コマンド **utils dbreplication status** を実行し、障害がいつ、どこで発生したかを検出します。

- 4 = 複製セットアップが失敗した

電話機の概要

登録済み電話機の数、登録済み SIP 電話機の数、登録済み SCCP 電話機の数、一部登録済み電話機の数、および登録試行の失敗回数など、Cisco Unified Communications Manager のノードに関する情報を表示します。該当する場合、これにはクラスタ内のすべてのノードが含まれます。

Registered Devices

SIP 電話機の数、SCCP 電話機の数、および Unified CM に登録されている電話機の総数を表示します。[Past 1 Minute] 列には、過去 1 分間に登録または登録解除された電話機の差分を表示します。

Registration Issues

Unified CM のすべての電話機の登録に関する問題を表示します。[Failed Attempts] タブには電話機の登録に失敗した試行回数が表示され、[Partial Registration] タブには電話機が部分的に登録された数が表示されます。[Past 1 Minute] 列には、過去 1 分間の差分値が表示されます。

デバイスの概要

登録済み電話機デバイス、登録済みゲートウェイ デバイス、登録済みメディア リソース デバイスなど、Unified CM ノードに関する情報を表示します。[Device Summary] には、該当する場合は、クラスタ内のすべてのノードが含まれます。

Registered Phones

Unified CM クラスタに登録された電話機の総数が表示されます。[Past 1 Minute] には、過去 1 分間に登録された電話機の総数の差分が表示されます。

Registered Gateways

Unified CM クラスタに登録されたゲートウェイ（FXS、FXO、T1CAS および PRI）の総数が示されます。[Past 1 Minute] には、過去 1 分間で登録されたゲートウェイの総数の差分が表示されます。

Registered Media Resources

Unified CM クラスタに登録されたメディア リソース（MOH、MTP、XCODE および CFB）の総数が表示されます。[Past 1 Minute] には、過去 1 分間で登録されたメディア リソースの総数の差分が表示されます。

Registered Other Station Devices

Unified CM クラスタに登録されたその他の端末デバイスの総数が表示されます。[Past 1 Minute] には、過去 1 分間のその他の端末デバイスの総計の差分が表示されます。

Registered Services

電話機、ゲートウェイ、メディア リソース、その他の端末デバイスなど、デバイスのさまざまなすべてのタイプの詳細が表示されます。各タイプの詳細が別々に表示されます。

IM and Presence の概要

PE アクティブ JSM 会議

アクティブな JSM 会議のパフォーマンス カウンタの数には、Cisco Presence Engine と Cisco XCP Router 間でのクライアント エミュレーション 会議の数が含まれます。このカウンタの値は、ボックスのライセンス済みユーザ数と常に同じになる必要があります。

[Past 1 Minute] には過去 60 秒のカウンタ値の差分を表示します。

Active Calendar Subscriptions

[Number of Active Calendar Subscriptions] パフォーマンス カウンタには、ボックスで現在アクティブなカレンダ サブスクリプションの数が含まれます。

[Past 1 Minute] には過去 60 秒のカウンタ値の差分を表示します。

Incoming SIP Subscriptions

[Number of Active Inbound SIP Subscriptions] パフォーマンス カウンタには、IM and Presence Service ノードの Cisco XCP SIP Federation Connection Manager サービスによって維持されている、アクティブな受信 SIP サブスクリプションの現在の数が含まれます。IM and Presence Service ノードが SIP ドメイン間フェデレーションまたは SIP ドメイン内フェデレーションに設定されている場合に、このカウンタを監視します。

[Past 1 Minute] には過去 60 秒のカウンタ値の差分を表示します。

Outgoing SIP Subscriptions

[Number of Active Outbound SIP Subscriptions] パフォーマンス カウンタには、IM and Presence Service ノードで Cisco XCP SIP Federation Connection Manager サービスによって維持されている、アクティブな発信 SIP サブスクリプションの現在の数が含まれます。IM and Presence Service ノードが SIP ドメイン間フェデレーションまたは SIP ドメイン内フェデレーションに設定されている場合に、このカウンタを監視します。

SubscriptionsOut と SubscriptionsIn を組み合わせた合計カウントは、どの IM and Presence Service ノードでも 260,000 を超えないようにする必要があります。

[Past 1 Minute] には過去 60 秒のカウンタ値の差分を表示します。

Total Ad Hoc Chat Rooms

[Total Ad Hoc Group Chat Rooms] パフォーマンス カウンタには、ノードで現在ホストされているアドホック チャット ルームの総数が含まれます。

Note アドホック チャット ルームは、すべてのユーザがルームを離れると自動的に破棄されます。そのため、このカウンタの値は定期的に増減します。

[Past 1 Minute] には過去 60 秒のカウンタ値の差分を表示します。

Total Persistent Chat Rooms

[Total Persistent Chat Rooms] パフォーマンス カウンタには、ノードでホストされた常設チャット ルームの総数が含まれます。ルーム所有者が明示的に常設チャット ルームを破棄する必要があります。このカウンタは、常設チャットルームの総数が非常に多いかどうかを識別する場合や、いくつかの常設チャットルームが定期的には使用されなくなっているかどうかを識別するために監視できます。

[Past 1 Minute] には過去 60 秒のカウンタ値の差分を表示します。

Cisco Jabber の概要

Jabber Login Failures

Cisco Simple Object Access Protocol（SOAP）インターフェイスによって受信され、失敗したログイン要求の数を表します。1 分後に、カウンタには最後の 60 秒間のカウンタ値の差分が表示されます。

Current Connected Jabber or XMPP Clients

個々の IM and Presence Service サーバの Cisco XCP Connection Manager に接続されている XMPP クライアントの現在の数が含まれます。この数は、展開の使用パターンに基づいて増減します。この数値が予想されるユーザベースよりも高い場合、詳細な調査が必要になることがあります。1 分後に、カウンタには最後の 60 秒間のカウンタ値の差分が表示されます。

IM Packets Since Last Restart

すべてのユーザ上で IM and Presence Service ノードによって処理された IM パケットの合計数を表示します。1 分後に、カウンタには最後の 60 秒間のカウンタ値の差分が表示されます。

IM Packets in Last 60 Seconds

すべてのユーザ上で最後の 60 秒間に IM and Presence Service ノードによって処理された IM パケットの合計数。このカウンタは、60 秒ごとにゼロにリセットされます。TotalMessagePackets と同じ IM パケットをカウントするためのルールが適用されます。組

織内のビジー IM 時間を識別できるようにこのカウンタを監視します。1 分後に、カウンタには最後の 60 秒間のカウンタ値の差分が表示されます。

学習パターン

Learned Pattern レポートおよび Service Advertisement Framework（SAF）フォワーダ レポートは、コール制御ディスカバリ機能をサポートします。コール制御ディスカバリ機能を設定すると、Cisco Unified Communications Manager は、SAF ネットワークを使用するほかのリモート コール制御エンティティにそれ自体とホスト対象の DN パターンをアドバタイズします。同様に、これらのリモート呼制御エンティティは、Unified CM が番号分析で学習、挿入可能なホスト対象の DN パターンをアドバタイズします。

カラム	Description
パターン	リモート呼制御エンティティから学習されたパターンの名前が表示されます。
TimeStamp	ローカルの Unified CM が学習パターンとしてパターンをマークした日時が表示されます。
Status	学習パターンが到達可能または到達不能かどうかを示します。
Protocol	学習パターンへの発信コールに使用した SAF 対応トランクのプロトコルが表示されます。リモート コール制御エンティティに SAF 対応トランクに設定されている QSIG トンネリングがある場合は、データに、QSIG トンネリングが使用されたことが示されます。たとえば、この列には、H.323 とともに EMCA 表示されます。
AgentID	学習パターンをアドバタイズしたリモート コール制御エンティティの名前が表示されます。
IP Address	学習パターンをアドバタイズしたコール制御エンティティの IP アドレスが表示されます。また、コール制御エンティティがコールの待機に使用するポート番号を表示します。
ToDID	学習パターンのPSTN フェールオーバー設定を表示します。
CUCMNodeId	ローカルの Unified CM ノードの ID を表示します。

ポート モニタ

ポート モニタでは、各 Cisco Unity Connection ボイス メッセージング ポートのアクティビティをリアルタイムにモニタすることができます。この情報は、システムのポート数が多すぎるかまたは不十分かを判断するために役立ちます。

ポート モニタは、次の表に説明するような各ポートの情報を表示します。

フィールド	説明
ポート名（Port Name）	Cisco Unity Connection Administration ポートの表示名です。
発信者	着信コールの場合、発信者の電話番号です。
Called	着信コールの場合、電話がかかっている電話番号です。
理由	該当する場合は、コールがリダイレクトされた理由です。
Redir	コールがリダイレクトされた内線番号です。コールが複数の内線番号にリダイレクトされている場合、このフィールドには最後の内線番号の 1 つ前の内線番号が表示されます。
最後のリダイレクト	コールがリダイレクトされた最後の内線番号です。
アプリケーションのステータス	Cisco Unity Connection が発信者にしているカンバセーションの名前です。ポートでコールの処理が行われていない場合、ステータスは[アイドル（Idle）]と表示されます。
画面のステータス	カンバセーションが現在実行中のアクションです。ポートでコールの処理が行われていない場合、ステータスは [アイドル（Idle）] と表示されます。
カンバセーションのステータス	カンバセーションが実行中のアクションに関する特定の詳細です。ポートでコールの処理が行われていない場合、ステータスは [アイドル（Idle）] と表示されます。
ポートの内線番号	ポートの内線番号です。
接続先	Cisco Unified Communications Manager SCCP 統合に対しては、ポートが登録されている Cisco Unified Communications Manager ノードの IP アドレスおよびポート。

履歴トレンドの表示

履歴トレンド分析は、デフォルトで [System Summary] ダッシュボードの下位のダッシュレット（[CPU Usage]、[Virtual Memory Usage]、および [Common Partition Usage]）に対して有効になっています。トレンド ビュー グラフを表示するには、ダッシュレットの右下の [Zoom] をクリックします。

前提条件

すべてのデバイスが Cisco Prime Collaboration Assurance で管理対象状態になっている必要があります。クラスタの場合は、すべてのノードが管理対象状態になっている必要があります。

音声デバイス（Cisco Unified CM、Cisco Packaged Contact Center Enterprise、Cisco Unified Presence、Cisco Unity Connection、Cisco Media Sense、Cisco Finesse、Cisco Unified IC、および Cisco Unified Contact Center Express）の場合は、システム定義のダッシュボードと一緒に、デバイス関連のメトリックのトレンドも表示できます。

Cisco Prime Collaboration リリース 11.5 以降の場合

音声デバイス（Cisco Unified CM、Cisco Packaged Contact Center Enterprise、Cisco Unified Presence、Cisco Unity Connection、Cisco Media Sense、Cisco Finesse、Cisco Unified IC、Cisco Unified Contact Center Express、および Cisco Virtualized Voice Browser）の場合は、システム定義のダッシュボードと一緒に、デバイス関連のメトリックのトレンドも表示できます。

（注）

- デバイス関連のメトリックは、選択するデバイス タイプによって異なります。
- 履歴トレンド分析は、Cisco Unified CCE、Cisco Voice Portal、MCU/TPS、Cisco Unified Border Element、シスコ音声ゲートウェイ、Cisco Unified Communications Manager Express、ISDN ゲートウェイなどの非音声デバイスではサポートされていません。

[Trend] ダッシュボード

メトリックのトレンドを表示するには、[Dashboard] ドロップダウン リストから [Trend] を選択し、[Metrics Selection] ダイアログボックスからトレンドを有効にするメトリックを選択して [Add] をクリックします。任意の数のメトリックを選択できますが、デバイス タイプごとに最大 6 個までのメトリックを選択することをお勧めします。

また、次の操作を実行できます。

- データを、チャートまたは表形式のいずれかで表示する。
- [Merge] オプションをクリックして、2 つ以上のパフォーマンス メトリックについてトレンドを比較する。
- [Zoom] をクリックして、トレンド グラフを詳細ビューで表示する。このオプションは、履歴、1 時間ごとの平均、最大、および最小のデータを表示する場合に便利です。詳細ビューに表示されるズーム セレクタ グラフを使用して、選択した期間のトレンドを表示するためのグラフの時間枠（x 軸）のポインタを調整することができます。
- ユーザインターフェイスの右上にある [Add Graph]（+）ボタンを使用してトレンドを追加する。
- チャート タイプを変更する。

カスタム パフォーマンス ダッシュボードの作成

Cisco Prime Collaboration リリース 11.5 以降の場合

ホーム ページに、カスタマイズされたダッシュボードを追加できます。**[ネットワーク正常性の概要（Network Health Overview）]**>**[パフォーマンス（Performance）]**にグラフィカル ビュー（最大 6 カウンタ）または表形式のビュー（最大 50 カウンタ）のいずれかで追加することができます。デフォルトでは、グラフィカル ビューが有効になっています。カウンタの最小、最大、および平均の値も表示されます。

（注） カスタム ダッシュボードのすべてのメタデータはデータベースに格納されます。ただし、カウンタの値はデバイスからライブで取得され、キャッシュ メモリに保存されます。パフォーマンス ダッシュボードが 30 分以上開いていない場合は、ポーリングが停止し、次にカスタム ダッシュボードが起動されるときにキャッシュ メモリがクリアされます。カスタムダッシュボード カウンタの履歴傾向が有効になっている場合、ポーリングされたデータは、データベースに 7 日間保存されます。パージ ポリシーの詳細については、『Cisco Prime Collaboration Assurance ガイド- Advanced』の「」の章を参照してください。

グラフィカル ビューでは、ポーリング間隔に指定された数秒または数分ごとに、カウンタの現在の値を表します。線上の赤い点にマウスを合わせて、カウンタの値をヒントとして表示することもできます。

（注） カウンタの最小、最大、および平均の値をグラフィカル ビューで表示するには、[See Average] をクリックします。

次のことも実行できます。

- カスタム ダッシュボードへイベントを追加する。
- グラフィカル ビューと表形式のビューを切り替える。

（注） カスタマイズされたダッシュボードをグラフィカル ビューで作成する場合、または編集オプションを使用して表形式のビューからグラフィカル ビューに切り替える場合は、選択するカウンタの数が 6 以下であることを確認してください。カウンタの数が 6 を超えた場合、ダッシュボードをグラフィカル ビューで表示するには、超過したカウンタを削除しなければなりません。

カスタム ダッシュボードを作成するには:

ステップ 1 [Cluster] または [Device] ドロップダウン リストから製品とクラスタを選択します。

ステップ 2 [Dashboard] ドロップダウン リストの横にある **[+]** ボタンをクリックします。

ステップ 3 [カスタム ダッシュボード（Custom Dashboard）] ページで、dashboardname（**//dashboardname//**）を入力し、ポーリング間隔、ビュー、およびサーバを選択します。

カスタム パフォーマンス ダッシュボードからカスタム グラフの履歴データを収集できます。

Cisco Prime Collaboration リリース 11.6 以前の場合

（注） 異なるログインを持つ 2 人のユーザが同じダッシュボード名、クラスタ、カウンタの詳細を使用してカスタム ダッシュボードを作成した場合、または異なるダッシュボード名でクラスタとカウンタ グループの詳細が同じカスタムダッシュボードを作成した場合、それぞれのユーザに対して、誤りのあるダッシュボード詳細が表示されます。

Cisco Prime Collaboration リリース 12.1 以降の場合

（注） カスタム ダッシュボード名が **Custom-//dashboardname//** から **Custom-//dashboardname_loggedInUser//** に変更され、異なるユーザがそれぞれのダッシュボードの詳細を正しいデータで表示できるようになりましたが、ダッシュボード名、クラスタ名、およびカウンタグループの詳細は同じままです。

グラフィカル ビューでカスタム ダッシュボードの作成時に、選択したパフォーマンス カウンタの履歴傾向を有効にすることができます。カスタム ダッシュボードを表形式のビューで作成する場合、またはグラフィカル ビューから表形式のビューへ切り替える場合は、このオプションは無効です。グラフィカル ビューから表形式のビューに切り替えたときに、履歴傾向データが失われたことを示す警告メッセージが表示されます。

（注）
- [履歴傾向（Historical Trend）] オプションを有効にするには、ポーリング間隔を 60 秒以上にする必要があります。
- 10 個以上のコミュニケーション マネージャ ノードを含むメガクラスタがある場合、ポーリング間隔は 30 秒以上に設定する必要があります。

ステップ 4 [Select Performance Counters] ペインから適切なパフォーマンス カウンタを選択します。カウンタ グループを展開してカウンタを選択します。カウンタに対応するインスタンスが、[Select Instances] ペインに表示されます。

ステップ 5 インスタンスを選択して [Add] をクリックします。

（注） [Select Performance Counters] または [Select Instances] ペインで有効な検索オプションを使用して、カウンタ グループ、カウンタ、またはインスタンスに対して大文字/小文字を区別する検索を実行することもできます。

ステップ 6 [Create] をクリックします。

[Edit] および **[Delete]** ボタンを使用して、作成したカスタム ダッシュボードを編集または削除できます。新しいパフォーマンス カウンタ イベントの作成については、を参照してください。カスタム ダッシュボードからカスタム イベントを作成する場合は、クラスタの詳細を指定する必要はありません。

（注） [カスタム ダッシュボードの編集（Edit Custom Dashboard）] または [カスタム ダッシュボードの削除（Delete Custom Dashboard）] ダイアログボックスには、ダッシュボード名のみが表示されます。

ダッシュレットの右下にある [Zoom] リンクをクリックすると、パフォーマンス カウンタの [Trend View] グラフが表示されます。[Trend View] グラフで使用可能な [Export] オプションを使用して、CSV または PDF の形式で履歴傾向データをエクスポートすることができます。

[Merge] をクリックして、作成した 1 つ以上のダッシュレットに対して [Merge View] グラフを表示することもできます。収集した傾向データは 7 日間保管された後、消去されます。

（注） [Zoom] オプションと [Merge] オプションは、カスタム ダッシュボードで履歴傾向オプションが有効になっている場合のみ使用できます。

カスタマイズされたダッシュボードの追加

ホーム ページに、カスタマイズされたダッシュボードを追加できます。

また、次の操作を実行できます。

- 既存のダッシュレットを別のダッシュボードに追加します。
- ダッシュレットをドラッグアンドドロップして、ダッシュボードの下に移動します。

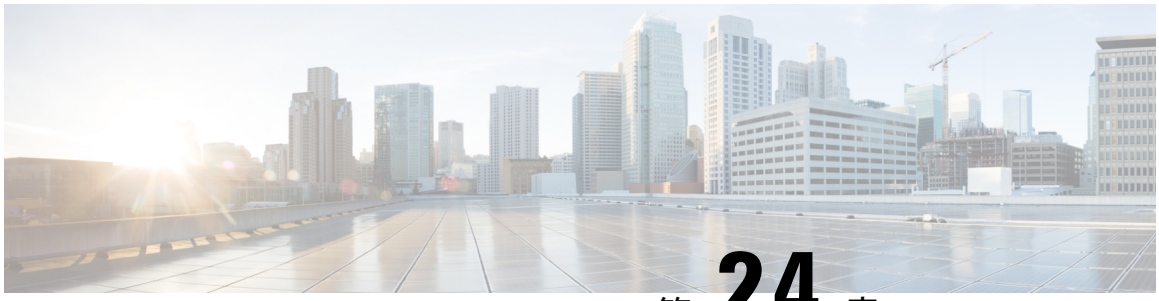
新規ダッシュボードを追加するには、次の手順を実行します。

ステップ 1 ホーム ページの右上隅にある [設定（Settings）]「」 アイコンをクリックし、[新規ダッシュボードの追加（Add New Dashboard）] をクリックします。

ステップ 2 表示されたボックスに任意の名前を入力し、[適用（Apply）] をクリックします。

ステップ 3 [Add Dashlet(s)] をクリックします。

ステップ 4 追加するダッシュレットの横にある [追加（Add）] をクリックします。



第 24 章

Cisco Prime Collaboration Assurance レポート

このセクションでは、次の点について説明します。

- Cisco Prime Collaboration Assurance レポート （467 ページ）
- Cisco Prime Collaboration Assurance レポートを生成するための前提条件 （468 ページ）
- CDR データ ソース コール詳細レコード NAM クレデンシャルの更新 （468 ページ）
- コール分類 （477 ページ）
- SFTP 設定項目の設定 （489 ページ）
- 管理レポート （494 ページ）
- CDR および CMR のコール レポート （495 ページ）
- NAM & Sensor Report （510 ページ）
- セッション レポート/会議レポート （520 ページ）
- TelePresence エンドポイント レポート （522 ページ）
- [CUCM レポートの起動（Launch CUCM Reports）] （524 ページ）
- その他のレポート （524 ページ）
- スケジュール済みレポート （530 ページ）
- 2,000 件を超えるレコードを含むレポートのデータへのアクセス （533 ページ）
- ファイルのダウンロードに関する問題のトラブルシューティング （534 ページ）

Cisco Prime Collaboration Assurance レポート

この章では、Cisco Prime Collaboration Assurance レポートのさまざまなレポートについて説明します。

Cisco Prime Collaboration Assurance レポートを生成するための前提条件

Cisco Prime Collaboration Assurance レポートを使用すると、問題領域を特定し、最も頻繁に使用されているエンドポイントと使用頻度の最も少ないエンドポイントを特定して、将来の展開で必要な場所とエンドポイントの種類を判断できます。

前提条件：

- データ ソースのクレデンシャルを更新します。「CDR データ ソース コール詳細レコード NAM クレデンシャルの更新」を参照してください。
- （ボイス コール レポート用の）コールを分類し、ダイヤルプランを追加して、ゲートウェイ コードを設定します。「コール分類」を参照してください。
- SFTP を設定します。「SFTP 設定項目の設定」を参照してください。
- Unified CM デバイスは、Managed の状態である必要があります。
- Cisco Prime Collaboration Assurance を、Unified CM で課金サーバとして追加する必要があります。

CDRデータ ソースコール詳細レコードNAMクレデンシャルの更新

Cisco Prime Collaboration Assurance は、Cisco Unified CM clusters または Cisco Prime Virtual Network Analysis Module（Prime vNAM）から、SCS（損失が 5 % を超えた秒数）コールの音声品質がユーザ定義の品質しきい値を満たしていない場合は、SNMP トラップを送信します。

Cisco Unified CM は、Cisco Voice Transmission Quality（CVTQ）アルゴリズムを使用して、コール全体の MOS 値を計算します。コールの終了時に、Cisco Unified CM はコール詳細レコード（CDR）と Call Management Records（CMRs）にデータを保存します（CDR と CMR の詳細については、『Cisco Unified Communications Manager コール詳細レコード アドミニストレーション ガイド』を参照してください）。

Unified Communications Manager パブリッシャ サーバにクレデンシャルを提供するには、次の手順を実行します。

- Cisco Prime Collaboration Assurance にクレデンシャルを提供する。
- クレデンシャルを最新の状態に保つ（Unified Communications Manager パブリッシャ サーバのクレデンシャルを更新するときは常に、Cisco Prime Collaboration Assurance の対応するクレデンシャルも更新する）。

クレデンシャルを更新するには、 **[CDS ソース設定（CDR Source Settings）]** > **[通話品質データソース管理（Manage Call Quality Data Sources）]**。

Cisco Prime Collaboration リリース 11.5 以降の場合

クレデンシャルを更新するには、**[アラームおよびレポートの管理（Alarm & Report Administration）]** > **[CDS ソース設定（CDR Source Settings）]** > **[通話品質データソース管理（Manage Call Quality Data Sources）]**。

Cisco Prime Collaboration リリース 12.1 SP3 以降の場合

クレデンシャルを更新するには、[**インベントリ（Inventory**）]> [**インベントリ管理（Inventory Management**）] > [**NAM の設定（Configure NAM**）] を選択します。

Prime NAM へのデータ ソースのクレデンシャルの追加

Prime NAM サーバにクレデンシャルを追加するには、次のようにします。

ステップ 1 選択 **[アシュアランス管理（Assurance Administration）]** > **[CDR Source Settings]** > **[Manage Call Quality Data Sources]**。

Cisco Prime Collaboration リリース 11.5 以降の場合

移行方法 **[アラームおよびレポートの管理（Alarm & Report Administration）]** > **[CDS ソース設定（CDR Source Settings）]** > **[通話品質データソース管理（Manage Call Quality Data Sources）]**。

Cisco Prime Collaboration リリース 12.1 SP3 以降の場合

移行方法 **[インベントリ（Inventory）]** > **[インベントリ管理（Inventory Management）]** > **[NAMの設定（Configure NAM）]**。

ステップ 2 [追加（Add）] をクリックし、必要なデータを入力します。ここでは、すべてのフィールドが必須です。

ステップ 3 [OK] をクリックします。

Cisco Prime Collaboration リリース 12.1 SP3 以降の場合

[保存（Save）] をクリックします。

（注） ホスト名または IP アドレスを、指定された形式で入力してください。ホスト名は必ず IP アドレスで解決可能でなくてはなりません。解決可能でない場合は、エラーメッセージが表示されます。[NAMの設定（Configure NAM）] ウィザードには、NAM 設定の [ステータス（Status）] が、[ステータス理由（Status Reasons）]と共に表示されます。ステータスには、成功、検証、および失敗があります。

ステップ 4 [更新（Refresh）] ボタンをクリックすると、クレデンシャルの情報がユーザ インターフェイスに反映されます。

クレデンシャルを編集または削除するには、選択したクレデンシャルのチェックボックスをオンにしてから、[編集（Edit）] または [削除（Delete）] をクリックします。

Cisco Prime Collaboration リリース 12.1 SP3 以降の場合

[更新（Refresh）] アイコンをクリックして、最新の NAM クレデンシャル ステータスを表示します。

クレデンシャルを編集するには、選択したクレデンシャルのチェックボックスをオンにして、必要な変更を行います。

（注） [選択数/<行の合計数>（Selected count/<total number of rows>）]：選択した行数を、テーブルの行の合計数で割った値が表示されます。

複数の Prime NAM クレデンシャルの削除

ステップ 1 **[インベントリ（Inventory）] > [インベントリ管理（Inventory Management）] > [NAM の設定（Configure NAM）]** の順に選択します。

ステップ 2 選択したクレデンシャルのチェックボックスをオンにします。

ステップ 3 [Delete] をクリックします。

選択した NAM を削除するかどうかを確認するメッセージがポップアップ表示されます。

（注） NAM の削除中にエラーが発生した場合は、ログを確認します。

複数の Prime NAM クレデンシャルの確認

ステップ 1 **[インベントリ（Inventory）] > [インベントリ管理（Inventory Management）] > [NAM の設定（Configure NAM）]** の順に選択します。

ステップ 2 クレデンシャルを確認する NAM を選択します。

ステップ 3 [Verify（検証）] をクリックします。

（注） NAM が [Verifying（Verifying）]「」 の状態にある間は、NAM を [検証（Verify）] または [削除（Delete）] できます。NAM を検証または削除しようとすると、NAM が [Verifying（Verifying）]「」 の状態にあるときに NAM のクレデンシャルを削除または検証できないことを示すメッセージが表示されます。

複数の NAM クレデンシャルの追加

複数の NAM クレデンシャルを追加するには、Prime NAM の詳細を含む CSV ファイルをインポートします。

CSV（コンマ区切り値）形式は、スプレッドシートとデータベースの最も一般的なインポートおよびエクスポート形式です。

CSV ファイルの準備

CSV ファイルは、デフォルトの Microsoft Excel スタイルの CSV ファイルに基づいています。CSV ファイルには、それぞれに多数の列がある、多数の行が含まれています。フィールドはコンマで区切られており、コンマや改行など、文字どおり処理する必要があるコンテンツは引用符で囲みます。

CSV ファイルの要件

CSV ファイルには、「よく整えられた形式」以外にも、次の要件があります。

各 CSV ファイルには、1 つのヘッダー行があります。

CS ファイルをインポートする場合は、CSV ファイルのヘッダー行を使用して、CSV ファイルの 2 行目以降のデータをデータベース内のフィールドにマップする方法を決めます。

ヘッダー行は、区切り記号（各列を区切るコンマを除く）を含めないようにする必要があり、これを行わないとインポータが正しく機能しない場合があります。

CSV は、6 ヘッダーと 7 ヘッダーの 2 種類のヘッダー ファイル形式をサポートしています。

- 12.1 以前のバージョンでは、ホスト名と IP アドレスが 2 つの異なるフィールドであったため、7 ヘッダー形式になっていました。
- 12.1 Service Pack 3 では、1 つのフィールドでホスト名と IP アドレスの両方をサポートするため、6 ヘッダー形式になっています。

CSV ファイルには、各 Prime NAM サーバで次の詳細情報を含める必要があります。

HostName を含む 6 ヘッダー ファイル形式の CSV

DisplayName	HostName	プロトコル	ポート	ユーザ名	Password
nam	nam.atlas.local	HTTP	80	admin	Atlas!123

IPAddress を含む 6 ヘッダー ファイル形式の CSV

DisplayName	IPAddress	プロトコル	ポート	ユーザ名	Password
NAM	10.104.243.11	HTTP	80	admin1	Nam!123

12.1 Service Pack 3 以降では、NAM のインポートでは 6 ヘッダー ファイル形式の使用が推奨されています。11.6 以前のバージョンでインポートされたファイルがある場合、同じヘッダー ファイルは 12.1 Service Pack 3 以降のリリースで再度使用することができます。

（注）
- 行が空白のままであり、各レコードが 1 行になっていることを確認します。
- 先頭と末尾の空白文字は無視されます。
- 改行が埋め込まれています。
- ホスト名は IP アドレスへと解決できる必要があります。

Prime NAM クレデンシャルのインポート

ステップ 1 **[インベントリ（Inventory）] > [インベントリ管理（Inventory Management）] > [NAM の設定（Configure NAM）]** の順に選択します。

ステップ 2 [NAMのインポート（Import NAM）] セクションで、[ファイルの選択（Choose File）] ボタンをクリックしてローカルの csv ファイルを参照し、[インポート（Import）] をクリックして、NAM を CSV 形式でインポートします。

ステップ 3 [インポート（Import）] をクリックします。

ステップ 4 [更新（Refresh）] アイコンをクリックして、最新の NAM クレデンシャル ステータスを表示します。

ステップ 5 [保存（Save）] をクリックします。

クレデンシャル検証：エラー メッセージ

次の表は、クレデンシャル検証のエラー メッセージです。これらのメッセージは、NAM インポートの一部として導入されました。

成功/エラー メッセージ	状態	解決策
IMPORT_PROCESS_ SUCCESS_MESSAGE	すべての NAM レコードが正常にインポートされました	成功メッセージ

成功/エラー メッセージ	状態	解決策
IMPORT_PROCESS_ SKIPPED_FEW_RECORDS	次のいずれかの原因により失敗しました。	
	1.「すべての NAM レコードが正常にインポートされませんでした。レコードのホスト名を解決できませんでした。インポート ファイルを確認してください。問題が解決しない場合は、ログを確認してください」。	
	2.「すべての NAM レコードが正常にインポートされませんでした。レコードの IP アドレスを解決できませんでした。インポート ファイルを確認してください。問題が解決しない場合は、ログを確認してください」。	
	3.「すべての NAM レコードが正常にインポートされませんでした。レコードのホスト名または IP アドレスを解決できませんでした。インポート ファイルを確認してください。問題が解決しない場合は、ログを確認してください」。	
IMPORT_PROCESS_FAILURE	「すべての NAM レコードが正常にインポートされませんでした。インポート ファイルを確認してください。問題が解決しない場合は、ログを確認してください」。	重複するものがないか確認し、IP アドレスなどの正しいデータを入力します。
INCORRECT_FILE_FORMAT	「インポートされたファイルの形式が正しくありません。正しい形式についてはユーザ ガイドを確認し、ファイルを CSV 形式のみでインポートしてください」。	ファイルを CSV 形式でのみインポートしてください。

成功/エラー メッセージ	状態	解決策
IMPORT_FILE_ HEADERS_EMPTY	「ファイル ヘッダーが正しくありません。正しい形式については、ユーザ ガイドを確認してください」。	正しいヘッダーを含むファイルを選択してください。
IMPORT_FILE_ CONTENT_EMPTY	「インポートされたファイルのコンテンツが空であるか、適切ではありません。正しい形式については、ユーザ ガイドを確認してください」。	NAMデータを入力してください。

複数のデータ ソース クレデンシャルの追加

複数のデータ ソース クレデンシャルを追加するには、Prime NAM または クラスタの詳細を含む csv ファイルをインポートします。

csv ファイルには、各 Prime NAM サーバまたは Cisco Unified CM サーバの以下の詳細が含まれている必要があります。

- 表示名
- IP アドレス
- ホスト名
- プロトコル
- ユーザ名
- [パスワード（Password）]

複数の Prime NAM または クラスタのクレデンシャルを追加するには、次のようにします。

ステップ 1 移行方法 **[アシュアランス管理（Assurance Administration）]** > **[CDS ソース設定（CDR Source Settings）]** > **[通話品質データ ソース管理（Manage Call Quality Data Sources）]**。

Cisco Prime Collaboration リリース 11.5 以降の場合

移行方法 **[アラームおよびレポートの管理（Alarm & Report Administration）]** > **[CDS ソース設定（CDR Source Settings）]** > **[通話品質データ ソース管理（Manage Call Quality Data Sources）]**。

ステップ 2 [インポート（Import）] をクリックします。

ステップ 3 **[インポート（Import）]** ダイアログボックスで、ローカル csv ファイルを参照し、**[インポート（Import）]** をクリックします。

ステップ 4 **[更新（Refresh）]** ボタンをクリックすると、クレデンシャルの情報がユーザインターフェイスに反映されます。

NAM クレデンシャルを使用した問題のトラブルシュートとクレデンシャルの確認

Cisco Prime Collaboration Assurance に問題が発生し、NAM にコンタクトまたは接続できなくなると、コールデータと設定データの収集や分析が中断される場合があります。その場合は、次を行ってください。

- クレデンシャルが有効であり、Cisco Prime Collaboration Assurance がアクティブにデータを取得していることを確認します。
- NAMの クレデンシャル ステータスやレポートに問題（時間差が著しいなど）があると思われる場合は、トラブルシュートを行ってください。

ステップ 1 次のトラブルシュートを行います。

Cisco Unified CM の場合: 次の操作を実行します。

- Cisco Unified CM のクラスタのクレデンシャルが、Cisco Prime Collaboration Assurance のクレデンシャルと一致し、（必要に応じて）正しいことを確認します。
- DNS パラメータが Cisco Prime Collaboration Assurance サーバで正しく指定されていること、および Cisco Unified CM ホスト名が DNS に追加されていることを確認します。（Cisco Prime Collaboration Assuranceは、正しい名前を取得するために、Cisco Unified CM の IP アドレスを解決できる必要があります）。
- クラスタと Cisco Prime Collaboration Assurance の間で、正常なデータ交換を妨げる既知の問題があるかどうかをチェックします。
- この問題は、Cisco Prime Collaboration Assurance と Cisco Unified CM の間の接続が切れた後に、再度確立した後で発生する可能性があります。Cisco Unified CM は、最初に古いファイルを Cisco Prime Collaboration Assurance に送信します。
- Cisco Prime Collaboration Assurance が依存しているクレデンシャルは、Cisco Unified CM プラットフォームで変更される可能性があります。この問題が発生した場合は、Unified CM の管理者に問い合わせて、正しいクレデンシャルを取得してください。必要に応じて、Cisco Prime Collaboration Assurance でクレデンシャルを更新します。

ステップ 2 クレデンシャルを確認します。

a) 移行方法 **[アシュアランス管理（Assurance Administration）]** > **[CDR ソース設定（CDR Source Settings）]** > **[通話品質データソース管理（Manage Call Quality Data Sources）]**。

Cisco Prime Collaboration リリース 11.5 以降の場合

移行方法 **[アラームおよびレポート管理（Alarm & Report Administration）] > [CDS ソース設定（CDR Source Settings）] > [通話品質データ ソース管理（Manage Call Quality Data Sources）]**。

Cisco Prime Collaboration リリース 12.1 SP3 以降の場合

[インベントリ（Inventory）] > [インベントリ管理（Inventory Management）] > [NAM の設定（Configure NAM）] の順に選択します。

b) クレデンシャルを確認する NAM を選択します。
c) [Verify（検証）] をクリックします。

データ ソース クレデンシャルを使用した問題のトラブルシューティングおよびクレデンシャルの確認

Cisco Prime Collaboration Assurance によるデータ ソースへのアクセスや接続を妨げる問題が発生すると、コールデータと設定データの収集と分析が中断される場合があります。[Data Source Management] ページの情報を使用すると、次のことができます。

- クレデンシャルが有効であり、Cisco Prime Collaboration Assurance がアクティブにデータを取得していることを確認します。
- データ ソース クレデンシャルやレポートに問題の可能性が見られる場合（時間差が著しい場合など）にトラブルシューティングを行う。

ステップ 1 詳細情報を表示するには、[データソース管理（Data Source Management）] ページで、[ステータス（status）] リンクをクリックします。

表示される情報には、問題の詳細や、トラブルシューティングの必要性の有無が記録されている場合があります。

ステップ 2 次のトラブルシュートを行います。

Cisco Unified CM の場合: 次の操作を実行します。

- Cisco Prime Collaboration Assurance とクラスタとの最後に成功した通信が最近のものであることを確認します。前回の通信ステータスが成功であっても、場合によっては、Cisco Prime Collaboration Assurance はデータを受信しているのではなく、データ受信を待機しているだけという可能性があります。
- Cisco Unified CM のクラスタのクレデンシャルが、Cisco Prime Collaboration Assurance のクレデンシャルと一致し、（必要に応じて）正しいことを確認します。
- DNS パラメータが Cisco Prime Collaboration Assurance サーバで正しく指定されていること、および Cisco Unified CM ホスト名が DNS に追加されていることを確認します。（Cisco Prime Collaboration Assuranceは、正しい名前を取得するために、Cisco Unified CM の IP アドレスを解決できる必要があります）。

- クラスタと Cisco Prime Collaboration Assurance の間で、正常なデータ交換を妨げる既知の問題があるかどうかをチェックします。
- Cisco Prime Collaboration Assurance がデータを破棄しているとコール データ ステータスが示している場合は、待機するか、予防措置を実施します。Cisco Prime Collaboration Assurance は、Unified CM 6.x 以降から古いデータを受信するとデータを破棄します。この問題は、Cisco Prime Collaboration Assurance と Cisco Unified CM の間の接続が切れた後に、再度確立した後で発生する可能性があります。Cisco Unified CM は、最初に古いファイルを Cisco Prime Collaboration Assurance に送信します。
- Cisco Prime Collaboration Assurance が依存しているクレデンシャルは、Cisco Unified CM プラットフォームで変更される可能性があります。この問題が発生した場合は、Unified CM の管理者に問い合わせて、正しいクレデンシャルを取得してください。必要に応じて、Cisco Prime Collaboration Assurance でクレデンシャルを更新します。

ステップ 3 クレデンシャルを確認します。

a) 移行方法 **[アシュアランス管理（Assurance Administration）]** > **[CDS ソース設定（CDR Source Settings）]** > **[通話品質データ ソース管理（Manage Call Quality Data Sources）]**。

Cisco Prime Collaboration リリース 11.5 以降の場合

移行方法 **[アラームおよびレポート管理（Alarm & Report Administration）]** > **[CDS ソース設定（CDR Source Settings）]** > **[通話品質データ ソース管理（Manage Call Quality Data Sources）]**。

b) クレデンシャルを確認するデータ ソースを選択します。

c) [確認（Verify）] をクリックします。

コール分類

Cisco Prime Collaboration Assurance では、コール分類を使用して、コール詳細レコード（CDR）レポートのコールを分類します。

Cisco Prime Collaboration Assurance は、次のデータを分析して、コールがシステム定義のコール カテゴリに該当するかどうかを判別します。

- CDR からの詳細
- ソース エンドポイントとターゲット エンドポイントのデバイス タイプ。
- コールの方向（着信または発信）
- プロトコル（H.323、MGCP、または SIP）

（注） 7 日より古い CDR レポートはパージされます。

次の表では、コールカテゴリのタイプと名前の一覧を示し、各カテゴリタイプに含まれるコールについて説明します。

カテゴリ タイプ	説明	カテゴリ名
ボイスメール	ボイスメールとの間でのコール。	Unity Voicemail：ボイスメールコールのシステム定義基準を満たすコール。Cisco Unity や Cisco Unity Connection との間で送受信されるコールなどが該当します。 （注） このカテゴリタイプにユーザ定義のカテゴリ名を追加することができます。
会議	会議システムとの間で送受信されるコール。	Conference Bridge：会議ブリッジを使用するコールのシステム定義基準を満たすコール。 （注） このカテゴリタイプにユーザ定義のカテゴリ名を追加することができます。
ICT	クラスタ間トランク（ICT）との間で送受信されるコール。	• ICT GK Controlled：ゲートキーパーにより制御される ICT コール。 • ICT Non-GK Controlled：ゲートキーパーにより制御されない ICT コール。
VG/Trunk-Outgoing	音声ゲートウェイまたはトランクへのコール。オフネットコールのみが対象となります。 （注） ユーザ定義ダイヤルプランは、VG/Trunk-Outgoing コール カテゴリのコールに適用されます。	• MGCP Gateway Outgoing：MGCP 音声ゲートウェイへのコール。 • H.323 Gateway Outgoing：H.323 音声ゲートウェイへのコール。 • H.323 Trunk Outgoing：H.323 トランクへのコール。 SIP Trunk Outgoing：SIP トランクへのコール。

VG/Trunk-Incoming	音声ゲートウェイまたはトランクへのコール。オフネットコールのみが対象となります。	• MGCP Gateway Incoming：MGCP 音声ゲートウェイからのコール。 • H.323 Gateway Incoming：H.323 音声ゲートウェイからのコール。 • H.323 Trunk Incoming：H.323 トランクからのコール。 SIP Trunk Incoming：SIP トランクからのコール。
Tandem	タンデム コールは、両方のエンドポイントが音声ゲートウェイまたはトランクである場合に発生します。	Tandem
OnNet Trunk	一方のエンドポイントがトランクであり、オフネット コールではないコール。 たとえば、トランクは Webex または PBX への接続に使用することができます。	• OnNet H.323 Trunk。 • OnNet SIP Trunk。
内部	上記のどのカテゴリにも該当しないコール。たとえば、一方のエンドポイントが IP フォンで、もう一方のエンドポイントが音声ゲートウェイであり、オフネット コールではないコールなどが該当します。	内部。
不明	システム関連の理由により、Prime Collaboration でエンドポイントのデバイス タイプを特定できませんでした。	不明。

次のような場合、Cisco Prime Collaboration Assurance は、ユーザ定義のコール カテゴリにコールを配置します。

- コールがすでに内部、VG/Trunk-Outgoing、または OnNet Trunk コールとして分類されている。
- ユーザ定義ダイヤル プランがコールが発生したクラスタに割り当てられている。

OffNet および OnNetNet コールを理解する

少なくとも一方のエンドポイントがゲートウェイまたはトランクで、そのエンドポイントが次のいずれかを満たす場合、コールはオフネットと見なされます。

- [Call Classification] パラメータは、Unified CM（管理）のゲートウェイ設定またはトランク設定で OffNet に設定されています。
- Unified CM では、次の両方の条件を満たしています。

  [Call Classification] パラメータがゲートウェイの設定またはトランクの設定で [System Default] に設定されている。

  [System Default] サービス パラメータが [Offnet] に設定されている。
- エンドポイントがアナログ ゲートウェイである。

オフネット コールの基準を満たさないコールはすべてオンネット コールと見なされます。

コール カテゴリの作成

ダイヤル パターンをダイヤル プランに追加するときに、コール カテゴリ名を作成することができます。

コール カテゴリを追加するには、次のオプションを選択します。 **[CDR分析の設定（CDR Analysis Settings）] > [コールカテゴリの設定（Set Call Category）]**。

Cisco Prime Collaboration リリース 11.5 以降の場合

移行方法 **[アラームとレポートの管理（Alarm & Report Administration）] > [CDR分析の設定（CDR Analysis Settings）] > [コールカテゴリの設定（Set Call Category）]**。

Cisco Prime Collaboration リリース 12.1 SP3 以降の場合

コール カテゴリを追加するには、**[アラームとレポートの管理（Alarm & Report Administration）] > [CDR分析の設定（CDR Analysis Settings）] > [コールカテゴリの設定（Set Call Category）]** を選択します。

Cisco Prime Collaboration Assurance では、いくつかの定義済みのコール カテゴリのセットがサポートされています。これらは、Cisco Prime Collaboration Assurance でコール カテゴリがどのように使用されるかを決定するものです。

定義済みのコール カテゴリのセットには、Unity ボイスメール（Unity Voicemail）、ローカル（Local）、長距離（Long Distance）、国際（International）、緊急（Emergency）、サービス（Service）、および無料通話（Toll Free）があります。

カスタム コール カテゴリの作成

Cisco Prime Collaboration Assurance では、カスタム コール カテゴリを作成することもできます。

ステップ 1 **[アラームとレポートの管理（Alarm & Report Administration）]** > **[CDR分析の設定（CDR Analysis Settings）]** > **[コールカテゴリの設定（Set Call Category）]** の順にクリックします。

ステップ 2 [追加（Add）] をクリックして、カスタム コール カテゴリを作成します。テーブルの最後に新しい行が表示されます。

ステップ 3 ドロップダウンから [コールカテゴリの種類（Call Category Type）] を選択します。

ステップ 4 **[保存（Save）]** をクリックします。

新しいコールカテゴリを作成して、そのチェックボックスをオンにすると、既存のコールカテゴリを変更したり、複数のチェックボックスをオンにして、コール カテゴリを [削除（Delete）] したりできます。

ダイヤル プランの追加

ダイヤルプランには一意の名前が必要です。フリーダイヤル番号のセットを登録することもできますが、ダイヤル パターンのセットを必ず登録する必要があります。ダイヤル パターンではコール カテゴリの名前とタイプが識別されています。ダイヤル パターンで指定されているルールまたはパターンと電話番号が一致すると、コールは該当するカテゴリに分類されます。

Cisco Prime Collaboration Assurance では、デフォルトのダイヤルプランが提供されます。これを基にして、独自のダイヤルプランを定義できます。デフォルトダイヤルプランには、デフォルトのダイヤル パターン（コール カテゴリの名前、タイプ、ルール）があります。ダイヤル プランを設定すると、コール カテゴリを更新し、デフォルトのダイヤルプランで指定されたルールの追加、変更、および削除を行うことができます。

ダイヤルプランは複数作成することができます。1 つのクラスタに割り当てることができるダイヤル プランは 1 つだけですが、同じダイヤル プランを複数のクラスタに割り当てることはできます。

Cisco Prime Collaboration リリース 11.5 以前の場合

ダイヤルプランを追加するには、次のオプションを選択します。 。

Cisco Prime Collaboration リリース 11.5 以降の場合

ダイヤルプランを追加するには、次のオプションを選択します。 **[アラームおよびレポート管理（Alarm & Report Administration）]** > **[CDR 分析の設定（CDR Analysis Settings）]** > **[ダイヤル プランの設定（Dial Plan Configuration）]**。

ダイヤル プランを割り当てるには、次のオプションを選択します。 **[アラームおよびレポート管理（AlarmおよびReport Administration）]** > **[CDR 分析の設定（CDR Analysis Settings）]** > **[ダイヤル プランの設定（Dial Plan Configuration）]**。

デフォルトのダイヤル プランを理解する

ダイヤル プランの追加時に、デフォルト ダイヤル プランのコピーが表示され、更新できるようになります。次の操作を実行できます。

- 独自のコール カテゴリ名を定義する。ただし、利用可能なコール カテゴリ タイプから選択する必要があります
- 既存のコール カテゴリ名から選択する。
- ダイヤル パターンを追加、更新、または削除する

Cisco Prime Collaboration リリース 12.1 SP3 以降の場合

- 既存のコール カテゴリ名から選択する。
- ダイヤル パターンを追加、更新、または削除する

ダイヤル プランの設定中の変更は、デフォルト ダイヤル プランには影響しません。デフォルト ダイヤル プランは北米番号計画（NANP）に基づいています。

次の表に、デフォルトのダイヤル プラン値を示します。

状態	文字数	デフォルト パターン	コール カテゴリ名	コール カテゴリ タイプ	説明	プライオリティ
>	3	011!	国際	国際	ダイヤルされた番号が 3 桁より長く、011 で始まっている場合は、このコールは「国際」として分類されます。	1
=	7	!	ローカル	ローカル	ダイヤルされた番号が 7 桁で、パターンが！（1 桁以上、この例では 7 桁の番号）の場合、このコールは「ローカル」として分類されます。	2

=	10	T!	トール フリー	トール フリー	ダイヤルされた番号が 10 桁で、パターンが T!（1 桁以上、この例ではダイヤル プランで定義されているフリーダイヤル番号のいずれかで始まる 10 桁の番号）の場合、このコールは「トール フリー」として分類されます。	3
=	10	G!	ローカル	ローカル	ダイヤルされた番号が 10 桁で、パターンが G!（1 桁以上、この例では Cisco Prime Collaboration Assurance で定義されているゲートウェイ コードで始まる 10 桁の番号）の場合、このコールは「ローカル」として分類されます。	4

=	10	!	長距離	長距離	ダイヤルされた番号が 10 桁で、パターンが！（1 桁以上、この例では 10 桁の番号）の場合、コールは「長距離」として分類されます。	5
=	11	T!	トール フリー	トール フリー	ダイヤルされた番号が 11 桁で、パターンが T!（1 桁より長い。ここでは、ダイヤル プランで定義されているフリーダイヤル番号のいずれかで始まる 11 桁の番号）の場合、このコールは Toll Free として分類されます。	6

=	11	XG!	ローカル	ローカル	ダイヤルされた番号が 11 桁で、パターンが XG! （1 桁以上、この例では任意の数字 1 文字で始まり、Cisco Prime Collaboration Assurance で定義されているゲートウェイ コードが続く 11 桁の番号）の場合、このコールは Local として分類されます。	7
=	11	!	長距離	長距離	ダイヤルされた番号が 11 桁で、パターンが！（1 桁以上、この例では 11 桁の番号）の場合、コールは「長距離」として分類されます。	8

（注） Cisco Prime Collaboration Assurance では、クラスタに割り当てられているダイヤル プランでフリーダイヤル コードが定義されている場合、コールが「トールフリー」として分類されます。

ダイヤル プランにダイヤル パターンを追加

追加または編集するダイヤル パターンを、ダイヤル プランに追加することができます。

Cisco Prime Collaboration リリース 11.5 以前の場合

ステップ 1 選択 **[CDR分析の設定（CDR Analysis Settings）]** > **[ダイヤル プランの設定（Dial Plan Configuration）]**。[追加（Add）] をクリックします。

Cisco Prime Collaboration リリース 11.5 以降の場合

選択 **[アラームおよびレポート管理（Alarm & Report Administration）]** > **[CDR 分析の設定（CDR Analysis Settings）]** > **[ダイヤル プランの設定（Dial Plan Configuration）]**。[Add] をクリックします。

[ダイヤルパターンの追加（Add Dial Pattern）] ダイアログボックスが表示されます。

Cisco Prime Collaboration リリース 12.1 SP3 以降の場合

[アラームとレポートの管理（Alarm & Report Administration）] > **[CDR分析の設定（CDR Analysis Settings）]** > **[ダイヤルプランの設定（Dial Plan Configuration）]** の順に選択します。

名前を入力して、[ダイヤルプラン名（Dial Plan Name）] フィールドに新しいダイヤル プランを追加します。

表の最後で **+**（追加）をクリックして、ダイヤル パターンを追加します。

新しい行が作成されます。

ステップ 2 次の各フィールドにデータを入力して、ダイヤル パターンを作成します。

- [条件（Condition）]：文字の数に適用されます。次のいずれかを選択します。
  - 左向き矢印（& lt;）：未満
  - 右矢印（& gt;）：より大きい
  - 等号（=）：等しい
- [文字数（Number of Chars）]：プラス（+）、シャープ（#）、アスタリスク（*）、コンマ（,）、アットマーク（@）を含む、数字と数字以外の文字の合計数を入力します。ダイヤル パターンが適用される電話番号の文字数を表します。
- [パターン（Pattern）]：パターンを入力して、数字に適用します。次のようになります。
  - G は数字がゲートウェイ コードを表していることを示します。
  - T は、Cisco Prime Collaboration Assurance がダイヤル プランで設定されたフリーダイヤル番号と比較されることを示します。
  - ! は、複数の数字（1234 または 5551234 のように、長さが 1 桁より大きい任意の数字）を示します。
  - X は 1 桁の数値（0、1、または 9 など）を示します。
- **Cisco Prime Collaboration リリース 12.1 SP2 以降の場合**

  [コールカテゴリ名（Call Category Name）]：次のラジオボタンのいずれかを選択し、必要に応じてデータを指定します。

- [既存（Existing）]：既存のコール カテゴリ名を選択します。
- [新規（New）]：一意の名前を入力し、コールのカテゴリ タイプを選択します。

- **Cisco Prime Collaboration リリース 12.1 SP3 以降の場合**

  [コールカテゴリ名（Call Category Name）]：[コール カテゴリの設定（Set Call Category）]「」 ユーザ インターフェイスを使用して設定されたドロップダウン リストから、既存のコール カテゴリ名を選択します。

ステップ 3 [OK] をクリックします。

Cisco Prime Collaboration リリース 12.1 SP3 以降の場合

[保存（Save）] をクリックします。

行がテーブルに追加されます。

VG/トランクへの発信、内戦コール、OnNet トランク コールにダイヤル パターンを割り当てる

次の表に、ユーザ定義のダイヤル プランから、Internal、VG/Trunk-Outgoing、OnNet Trunk のコール カテゴリにダイヤル パターンを割り当てる方法を示します。

Cisco Prime Collaboration によって、このカテゴリ タイプのダイヤル パターンが割り当てられます。	適用先の電話番号の種類	対象となるコールのシステム定義カテゴリ
• 会議 • 緊急 • 国際 • ローカル • 長距離 • サービス • トール フリー • [ボイスメール（Voicemail）]	接続先	VG/Trunk-Outgoing
• 会議 • ボイスメール	送信元	

Cisco Prime Collaboration によって、このカテゴリ タイプのダイヤル パターンが割り当てられます。	適用先の電話番号の種類	対象となるコールのシステム定義カテゴリ
• 会議 • ボイスメール	• 送信元 • 送信先	• 内部 • OnNet Trunk

ダイヤル プランの編集

ダイヤル プランを編集できます。ダイヤル プランの編集中に、ダイヤル パターンの追加、編集、または削除を行うことができます。

ステップ 1 **[アラームとレポートの管理（Alarm & Report Administration）] > [CDR分析の設定（CDR Analysis Settings）] > [ダイヤルプランの設定（Dial Plan Configuration）]** の順に選択します。

ステップ 2 [編集（Edit）] アイコンをクリックして、ダイヤル パターンを変更します。

ステップ 3 必要な変更を加えます。

ステップ 4 既存のダイヤル パターンを変更するには、「「ダイヤル プランの追加」」の**ステップ 3** を行います。

ステップ 5 [保存（Save）] アイコンをクリックします。テーブルの行が更新されます。

ダイヤル プランの削除

ダイヤル プランを削除することができます。

ステップ 1 該当する行を選択して [削除（Delete）] ボタンをクリックすると、ダイヤル プランが削除されます。

ステップ 2 [保存（Save）] をクリックして、すべての変更をダッシュレットに保存します。

[キャンセル（Cancel）] をクリックして終了します。

ゲートウェイ コードの設定

Cisco Prime Collaboration Assurance は、設定されているゲートウェイ コードを使用して、外部コールのコール分類を決定します。

（注） ゲートウェイ コードがすでに設定されているゲートウェイを表示するには、クラスタを選択して [表示（View）] をクリックします。ゲートウェイ コード レポートには、メディア ゲートウェイ制御プロトコル（MGCP）、および H323 ゲートウェイのみが表示されます。アナログのシグナリング接続制御部（SCCP）ゲートウェイは表示されません。

ゲートウェイ コードを設定するには、次のようにします。

ステップ 1 移行方法 **[アシュアランス管理（Assurance Administration）]** > **[CDR分析の設定（CDR Analysis Settings）]** > **[ゲートウェイコードの設定（Gateway Code Configuration）]**。

Cisco Prime Collaboration リリース 11.5 以降の場合

移行方法 **[アラームおよびレポートの管理（Alarm & Report Administration）]** > **[CDR 分析の設定（CDR Analysis Settings）]** > **[ゲートウェイコードの設定（Gateway Code Configuration）]**。

ステップ 2 [ゲートウェイコード概要（Gateway Code Summary）] ページでクラスタを選択し、[ゲートウェイコードの管理（Manage Gateway Code）] をクリックします。

ステップ 3 ゲートウェイコードを入力し、[適用（Apply）] をクリックします。

SFTP 設定項目の設定

Unified Communications Manager を使用してコールを監視する場合は、SFTP を設定する必要があります。

SFTP を設定するには、次の手順を実行します。

ステップ 1 移行方法 **[アシュアランス管理（Assurance Administration）]** > **[CDR ソース設定（CDR Source Settings）]** > **[CUCM SFTP クレデンシャル（CUCM SFTP Credentials）]**。

Cisco Prime Collaboration リリース 11.5 以降の場合

移行方法 **[アラームおよびレポート管理（Alarm & Report Administration）]** > **[CDR ソース設定（CDR Source Settings）]** > **[CUCM SFTP クレデンシャル（CUCM SFTP Credentials）]**。

Cisco Prime Collaboration リリース 12.1 以降の場合

移行方法 **[インベントリ（Inventory）]** > **[インベントリ管理（Inventory Management）]** > **[CUCM/SFTP クレデンシャル（CUCM/SFTP Credentials）]**。

Cisco Prime Collaboration リリース 12.1 SP3 以降の場合

移行方法 **[インベントリ（Inventory）]** > **[インベントリ管理（Inventory Management）]**。[CUCM SFTPクレデンシャル（CUCM SFTP Credentials）] タブをクリックします。

ステップ 2 必要な情報を入力します。フィールドの説明については、「[SFTP Settings] ページ - フィールドの説明」を参照してください。

ステップ 3 [適用（Apply）] をクリックします。
すべての Unified Communications Manager で SFTP パスワードを更新するかどうかを確認するポップアップウィンドウが表示されます。

ステップ 4 **[保存（Save）]** をクリックします。

管理対象のすべての Unified Communications Manager のパブリッシャ全体で SFTP クレデンシャルを更新するかどうかを確認するポップアップ メッセージ ウィンドウが表示されます。

（注） Cisco Prime Collaboration Assurance が、管理対象の Unified Communications Manager のパブリッシャで課金サーバとして追加されます。

ステップ 5 **[保存（Save）]** をクリックします。

管理対象のすべての Unified Communications Manager のパブリッシャ全体で SFTP クレデンシャルを更新するかどうかを確認するポップアップ メッセージ ウィンドウが表示されます。

（注） Cisco Prime Collaboration Assurance が、管理対象の Unified Communications Manager のパブリッシャで課金サーバとして追加されます。

ステップ 6 **[はい（Yes）]** をクリックします。

[SFTP Settings] ページ - フィールドの説明

Cisco Prime Collaboration リリース 12.1 SP3 以降の場合

次の表では、SFTP 設定ページのフィールドについて説明します。

表 *60 : [SFTP Settings]* ページ - フィールドの説明

フィールド	説明
[Username]	ユーザ名は smuser から変更できません。 これと同じ username と smuser をCisco Unified Communications Managerに設定する必要があります。

フィールド	説明
パスワード	新規インストール中は、CUCM SFTP クレデンシャルがデフォルトで設定されていないことを確認してください。**[インベントリ管理（Inventory Management）] -> [CUCM SFTP クレデンシャル（CUCM SFTP Credentials）]** タブで、CUCM SFTP パスワードを設定する必要があります。 クレデンシャルが設定されていない場合、ユーザはデバイス検出中に PCA を CDR 接続先として CUCM に追加することができません。アプリケーションは、CUCM SFTP パスワードを設定するようユーザに警告するために、「Please configure CUCM SFTP credentials to enable this feature. It can be configured under CUCM SFTP Credentials Tab」と表示します。 （注） PCA を CDR 接続先として CUCM に追加する必要がある場合は、デバイスの検出を開始するときに、[デバイスの検出（Discover Devices）] -> [デバイス検出（Device Discovery）] タブの [自動設定（Auto-Configuration）] オプションで、[Unified CMサーバでPrime CollaborationサーバをCDR接続先として追加する（Add the Prime Collaboration server as a CDR Destination in the Unified CM servers）] チェックボックスをオンにしてください。詳細については、「検出方法」のセクションを参照してください **Cisco Prime Collaboration リリース 12.1 SP3 以降の場合** デフォルトのパスワードは smuser です。ここでパスワードを変更する場合は、smuser のパスワードも Cisco Unified Communications Manager で変更する必要があります。
パスワードの再入力	確認のためにパスワードを入力します。

Cisco Prime Collaboration リリース 12.1 SP3 以降の場合

次の表では、SFTP 設定ページのフィールドについて説明します。

表 *61 : [SFTP Settings]* ページ - フィールドの説明

フィールド	説明
Low-Volume Schedule Hours	
<day> <timerange>	timerange は、各曜日について、Cisco Prime Collaboration Assurance プロセスが処理するレコードが少なくなってきた時間を示します。少量スケジュールの期間中、Cisco Prime Collaboration Assurance はデータベースのメンテナンスを実行します。
その他	
Wait for Diagnostic Report (min)	データが大量である場合、Cisco Prime Collaboration Assurance による検索時にここで指定した分単位の時間が経過すると、その時点までに検出された一致レコードが診断レポート用に表示されます。
Report Data Retention Period (days)	データをパージする前に、Cisco Prime Collaboration Assurance のデータベースに保持される日数。
SFTP	
[ユーザ名（Username）]	ユーザ名は smuser から変更できません。 これと同じ username と smuser をCisco Unified Communications Managerに設定する必要があります。

フィールド	説明
[Change password] チェックボックス	**Cisco Prime Collaboration リリース 12.1 SP3 以降の場合** 新規インストール中は、CUCM SFTP クレデンシャルがデフォルトで設定されていないことを確認してください。**[インベントリ管理（Inventory Management）] -> [CUCM SFTP クレデンシャル（CUCM SFTP Credentials）]** タブで、CUCM SFTP パスワードを設定する必要があります。 クレデンシャルが設定されていない場合、ユーザはデバイス検出中に PCA を CDR 接続先として CUCM に追加することができません。アプリケーションは、CUCM SFTP パスワードを設定するようユーザに警告するために、「Please configure CUCM SFTP credentials to enable this feature. It can be configured under CUCM SFTP Credentials Tab」と表示します。 （注） PCA を CDR 接続先として CUCM に追加する必要がある場合は、デバイスの検出を開始するときに、[デバイスの検出（Discover Devices）] -> [デバイス検出（Device Discovery）] タブの [自動設定（Auto-Configuration）] オプションで、[Unified CMサーバでPrime CollaborationサーバをCDR接続先として追加する（Add the Prime Collaboration server as a CDR Destination in the Unified CM servers）] チェックボックスをオンにしてください。詳細については、「検出方法」のセクションを参照してください **Cisco Prime Collaboration リリース 12.1 SP3 以降の場合** デフォルトのパスワードは smuser です。ここでパスワードを変更する場合は、smuser のパスワードも Cisco Unified Communications Manager で変更する必要があります。

管理レポート

利用可能な管理レポートは次のとおりです。

レポート	説明

System Status レポート	インベントリ、データ消去、通知、電話ライセンス（模擬テスト、電話ステータステスト、IP SLA 音声テストで構成）、およびシステム制限に関する情報を表示します。
	
	模擬テスト、電話ステータス テスト、および IP SLA 音声テストでは、次のテスト結果についてのみ情報が提供されます。
	• 模擬テスト：Cisco Prime Collaboration Assurance サーバの CPU 使用率が高いためにテストの実行に失敗した場合。
	• 電話ステータス：SAA ソース デバイスに到達できない場合。
	• IP SLA 音声テスト：
	  • 設定が正しくない場合。
	  • デバイスのメモリが不足している場合。
	  • ソース デバイスが応答していない場合。
	  • デバイスがリブートした場合。
	
	電話ステータス テストでは、次の結果について情報が提供されます。
	• 電話ステータステスト：SAA ソース デバイスに到達できない場合。
	
	システム制限のパラメータについては、次の説明が適用されます。
	• ポート：イーサネット ポートはこのパラメータに分類されます。
	• インターフェイス：音声インターフェイスはこのパラメータに分類されます。

レポート	説明
ログオンしているユーザ レポート	Cisco Prime Collaboration Assurance に現在ログインしているユーザを特定するために役立ちます。
プロセス ステータス	Cisco Prime Collaboration Assurance で現在実行されているプロセスのステータスを表示します。

CDR および CMR のコール レポート

Cisco Prime Collaboration Assurance で処理できるのは、過去 24 時間の CDR および CMR データだけです。CDR レポートは、コール カテゴリ タイプ、コール クラス、コール時間、コール リリース コードなどのコールの詳細を表示します。CMR レポートは [音声コール品質拠点上位5ヶ所（Top 5 Voice Call Quality Location）] からクロス起動でき、CDR レポートは [コール失敗発生拠点上位5ヶ所（Top 5 Call Failure Location）] からクロス起動できます。また、CMR レポートは ServiceQualityThresholdCrossed アラームからもクロス起動できます。レポートには、最初に最大 40 件のレコードがロードされ、下へスクロールするとさらに多くのレコードを表示できます。

生成されたレポートから任意のグレードを選択すると、その特定の CDR レコードについて、CMR レポートの詳細をインライン CMR（ポップオーバー）で確認できます。

（注） CDR レポートは、Cisco Prime Collaboration Assurance と CUCM の両方が同じドメイン内にある場合にのみ機能します。

CMR レポートでは、クラスタのすべてのコール データを含むレポート、またはコール データのサブセットを含むレポートが生成されます。

次の表では、CDR コール レポートのフィールドについて説明します。

フィールド	説明

Grade	音声コールのグレード設定に基づきます。次のいずれかを選択します。 • [良好（Good）]：コール値がロング コールの SCSR（%）またはショート コールの SCSR（%）のしきい値を下回っています。このグレードの値は緑色で表示されます。 • [可（Acceptable）]：コール値がロング コール SCSR（%）またはショート コールの SCSR (%) のしきい値以上です。このグレードの値はオレンジ色で表示されます。 • [不良（Poor）]：コール値がロング コールの SCSR（%）またはショート コールの（%）のしきい値を上回っています。このグレードの値は赤色で表示されます。 • [該当なし（N/A）]：SCSR（%）が利用不可能または負の値です。 • [すべて（All）]：すべてのグレードを選択します。
クラスタ ID	Unified Communications Manager クラスタです。

発信者/着信者	• **ディレクトリ番号**：コールが行われたディレクトリ番号です。 • **デバイス タイプ**：コールを発信したデバイスのタイプです。 • **シグナリング IP**：コール シグナリングを発信したデバイスの IP アドレスです。IP Phone の場合、このフィールドでは電話機のアドレスが指定されます。PSTN コールの場合、このフィールドでは H.323 ゲートウェイのアドレスが指定されます。 • **B チャネル**：MGCP ゲートウェイの B チャネル番号で、適用されない場合は NA となります。 • **メディア IP**：コールの発信元の IP アドレスです。 • **コーデック**：コーデック名です。 • **メディア ポート**：コールの発信元のポートです。 • **デバイス プール**：コールの発信元のデバイス プールです。 • **デバイスの場所**：コールの発信場所です。[表示（Show）] ドロップダウン メニューから [クイックフィルタ（Quick Filter）] を選択すると、Caller/Called のデバイスの場所の検索オプションを指定できます。 • [デバイス名（Device Name）]：デバイスの名前です。 • **終了原因**：コールが終了した理由を表す文字列です。

Caller Video/Called Video	• **ビデオコーデック**：ビデオコーデック名です。 • **ビデオ帯域幅**：ビデオの帯域幅です。 • **ビデオ IP**：ビデオの発信元の IP アドレスです。 • **ビデオ ポート**：ビデオの発信元のポートです。 • **ビデオ解像度**：ビデオの解像度です。
Call Class	次のいずれかです。 • Offnet • Onnet （**注**） 詳細については、OffNet および OnNetNet コールを理解する （480 ページ）を参照してください。
期間	コールが開始された日付と時刻を、Cisco Prime Collaboration Assurance サーバのローカル タイム ゾーン（Cisco Unified CM が配置されているタイム ゾーンではなく）で表します。最大時間の制限は 7 日間です。。
Call Duration(s)	コールの長さ（秒単位）。
Call Category Names	コールが属するカテゴリのカンマ区切りのリスト。詳細については、コール分類 （477 ページ）およびコール カテゴリの作成 （480 ページ）を参照してください。
Call Category Types	コール カテゴリが属するカテゴリ タイプのカンマ区切りのリスト。詳細については、次の項を参照してください：コール分類 （477 ページ）およびコール カテゴリの作成 （480 ページ）

次の表では、CMR レポートのフィールドについて説明します。

フィールド	説明
MOS	サンプル期間中の平均 MOS 値。サンプル期間が非常に短い場合、この値は N/A と表示されるか、または表示されません。 MOS はリスナー側の音質を反映します。

Minimum MOS	サンプル期間中の最小 MOS スコア。 サンプル期間が非常に短い場合、この値はN/Aと表示されるか、または表示されません。
Grade	音声コールのグレード設定に基づきます。次のいずれかを選択します。 • [良好（Good）]：コール値がロング コールの SCSR（%）またはショート コールの SCSR（%）のしきい値を下回っています。このグレードの値は緑色で表示されます。 • [可（Acceptable）]：コール値がロング コール SCSR（%）またはショート コールの SCSR (%) のしきい値以上です。このグレードの値はオレンジ色で表示されます。 • [不良（Poor）]：コール値がロング コールの SCSR（%）またはショート コールの（%）のしきい値を上回っています。このグレードの値は赤色で表示されます。 • [該当なし（N/A）]：SCSR（%）が利用不可能または負の値です。 • [すべて（All）]：すべてのグレードを選択します。

発信者/着信者	• **ディレクトリ番号**：コールが行われたディレクトリ番号です。 • **デバイス タイプ**：コールを発信したデバイスのタイプです。 • **シグナリング IP**：コール シグナリングを発信したデバイスの IP アドレスです。IP Phone の場合、このフィールドでは電話機のアドレスが指定されます。PSTN コールの場合、このフィールドでは H.323 ゲートウェイのアドレスが指定されます。 • **B チャネル**：MGCP ゲートウェイの B チャネル番号で、適用されない場合は NA となります。 • **メディア IP**：コールの発信元の IP アドレスです。 • **コーデック**：コーデック名です。 • **メディア ポート**：コールの発信元のポートです。 • **デバイス プール**：コールの発信元のデバイス プールです。 • **デバイスの場所**：コールの発信場所です。[表示（Show）] ドロップダウン メニューから [クイックフィルタ（Quick Filter）] を選択すると、Caller/Called のデバイスの場所の検索オプションを指定できます。 • [デバイス名（Device Name）]：デバイスの名前です。
リスナー DN/IP	MOS と障害の詳細が報告されたエンドポイント（着信側または発信側）を識別します。次のいずれかを示します。 • リスナーの IP アドレスです。 • リスナーの電話番号です。
Jitter (ms)	サンプル期間中のジッタ値（ミリ秒単位）。

Packet Loss	サンプル期間中にネットワーク伝送が原因で失われたパケットの数です。観察された RTP シーケンス番号の分析に基づいて計算されます。
Max Jitter (ms)	サンプル期間中の最大ジッタ値（ミリ秒単位）です。
フレーム損失発生秒数（Conceal Seconds）	音声ストリームの開始以降、隠蔽イベント（フレーム損失）があった秒数（深刻な隠蔽の秒数を含む）です。
深刻なフレーム損失発生秒数（Severely Conceal Seconds）	大量の（50 ミリ秒を超える）隠蔽が確認された秒数。
隠蔽フレーム	合計フレームに対する隠蔽フレームの比率です。
遅延	遅延
クラスタ	Unified Communications Manager クラスタです。
期間	コールが開始された日付と時刻を、Cisco Prime Collaboration Assurance サーバのローカル タイム ゾーン（Unified Communications Manager が配置されているタイム ゾーンではなく）で表します。
Call Duration(s)	コールの長さ（秒単位）。
Caller Termination Cause	発信側エンドポイントでコールが終了した理由を表す文字列。
Called Termination Cause	着信側エンドポイントでコールが終了した理由を表す文字列。失敗したコールの原因コードについては、『Cisco Unified Communications Manager コール詳細レコード アドミニストレーション ガイド』の「コール終了原因コード」の項を参照してください。

ビデオ属性	エンドポイント レポートには、次のようなビデオ属性が含まれています（ビデオ エンドポイントの場合）。 • ビデオの長さ • ビデオのパケット損失 • ビデオ ジッター • ビデオのラウンド トリップ時間 • ビデオの RX 解像度 • ビデオの RX フレーム損失
Severely Conceal Seconds Ratio (%)	音声品質を測定するメトリック。コールの合計時間に対する深刻な隠蔽の秒数（SCS）の比率を表します。
Conceal Seconds Ratio (%)	ネットワーク品質を測定するメトリック。コールの合計時間に対する隠蔽秒数（CS）の比率を表します。

（注）
- デフォルトでは、CDR および CMR レポートの一部の列は非表示になっています。他のフィールドを表示するには、[設定（settings）] ボタンをクリックし、[列（columns）] を選択します。
- CDR および CMR レポートは Jabber をサポートしています。

Cisco Prime Collaboration リリース 11.5 以降の場合

デバイスの場所をシステムの場所のいずれか（Hub_None、Phantom、または Shadow）に設定した場合、[場所（Location）] フィールドには、デバイスで設定されている場所ではなく、デバイス プールで設定されている場所が表示されます。

（注）

- Cisco Prime Collaboration Assurance は、Unified Communications Manager にユーザが定義した場所 Hub_None 表示して、次の機能 とレポートを提供します。
  - CDR および CMR レポート
  - 上位 5 位の低音声通話品質ロケーション
  - 上位 5 つの通話失敗の場所
  - 未登録の電話機のトラブルシューティング：上位 5 ヶ所
  - 場所ごとのグローバル検索
- デバイスの場所が Hub_None に設定されていて、Unified Communications Manager のユーザ定義のどのデバイス プールにも関連付けられていない場合は、Cisco Prime Collaboration Assurance で [デバイスの場所（Device Location）] が Hub_None として表示されます。また、Cisco Prime Collaboration Assurance では、場所ごとのグローバル検索および Unified Communications Manager のトラブルシューティング ビューで、Hub_None が有効な場所として表示されます。

クイック フィルタ オプションを使用すると、レポートのフィールドをフィルタ処理できます。詳細については、「フィルタ（Filters）」の「クイック フィルタ」の項を参照してください。

CDR および CMR レポートは、CSV と PDF のどちらの形式でもエクスポートできます。PDF ファイルにエクスポートできるレコードの最大数は 30,000 です。CSV ファイルにエクスポートできるレコードの最大数は 200,000 です。

レポートをエクスポートするには、レポート ウィンドウの右側のペインにある [エクスポート（Export）] ツール ボタンをクリックします。ファイルをエクスポートしようとしたときにクライアント システムが応答しない場合は、「ファイルのダウンロードに関する問題のトラブルシューティング」を参照してください。

CDR および CMR レポートでサポートされているビデオ コーデックは次のとおりです。

- AAC
- G711Alaw 56k
- G711Alaw 64k
- G711Ulaw 56k
- G711Ulaw 64k
- G722 48k
- G722 56k
- G722 64k
- G722.1 24k
- G722.1 32k

- G723.1
- G726 16K
- G726 24K
- G726 32K
- G728
- G729
- G729AnnexA
- G729AnnexAwAnnexB
- G729AnnexB
- GSM
- GSM Enhanced Full Rate
- GSM Full Rate
- GSM Half Rate
- iSAC
- H.264
- H.265

CDR & CMR レポートの生成

CDR および CMR のコール レポートを生成する手順を次に説明します。

（注） 管理者のみがCDR/CMR レポートをエクスポートできます。サーバにエクスポートするタスクを自動化するには、スクリプトを作成する必要があります。

ステップ 1 選択 **[アシュアランス レポート（Assurance Reports）]** > **[CDR および CMR レポート（CDR & CMR Reports）]**。

Cisco Prime Collaboration リリース 11.5 以降の場合

移行方法 **[レポート（Reports）]** > **[CDR および CMRレポート（CDR & CMR Reports）]** 。

[CDR&CMRレポート（CMR Reports）] ページが表示されます。

ステップ 2 以下に示すフィールドに情報を入力します。

表 *62 :*

フィールド	説明
ディスプレイ	[表示（Display）] から [CDR/CMR] を選択します
クラスタ	[クラスタ（Cluster）] から [クラスタ（Clusters）] を選択します。デフォルト値は「すべて（All）」です。
場所/デバイス プール	[Location/DevicePool] から [場所（Location）] または [デバイス プール（Devicepool）] を選択します。デフォルト値は「場所（ロケーション）」です。 [Location/DevicePool] から [場所（Location）] を選択した場合は、[場所（Location）] から任意の場所を選択します。[Location/DevicePool] から [デバイス プール（Devicepool）] を選択する場合は、[デバイス プール（Devicepool）] から任意のデバイス プールを選択します。[場所（Location）] または [デバイス プール（Devicepool）] で利用可能な検索オプションから Location/Devicepool を検索することもできます。[場所（Location）] または [デバイス プール（Devicepool）] のデフォルト値は任意です。
デバイス タイプ	[デバイス タイプ（Device Type）] からデバイスを選択します。デフォルト値は「すべて（Any）」です。
エンドポイント	[エンドポイント（Endpoint）] から、[ディレクトリ番号（Directory Number）] または [IP アドレス（IP Address）] を選択します。デフォルト値は「ディレクトリ番号（Directory Number）」です。
発信者	ディレクトリ番号または発信者の IP アドレスを入力します。ディレクトリ番号のデフォルト値は「*」で、IP アドレスのデフォルト値は「*.*.*.*.」です。 ディレクトリ番号には、英数字と特殊文字（+、*、@、_、-など）の任意の組み合わせを含めることができます。 ディレクトリ番号検索の際、1 桁のワイルドカードには大文字の「X」を使用します。複数桁のワイルドカードには「*」を使用してください。例としては「1100X」や「11*」などです。 IP アドレス検索の場合、「*」ワイルドカードはオクテット全体に適用されます。たとえば、「172.30.*.*」や「2005:0420:2e00:0094:*:*:*:*.」となります。

フィールド	説明
コール済み	ディレクトリ番号または発信者のIPアドレスを入力します。ディレクトリ番号のデフォルト値は「*」で、IPアドレスのデフォルト値は「*.*.*.*.」です。 ディレクトリ番号には、英数字と特殊文字（+、*、@、_、-など）の任意の組み合わせを含めることができます。 ディレクトリ番号検索の際、1桁のワイルドカードには大文字の「X」を使用します。複数桁のワイルドカードには「*」を使用してください。例としては「1100X」や「11*」などです。 IPアドレス検索の場合、「*」ワイルドカードはオクテット全体に適用されます。たとえば、「172.30.*.*」や「2005:0420:2e00:0094:*:*:*:*.」となります。
Call Category	[コールカテゴリ（Call Category）] から、名前またはタイプを選択します。デフォルト値は「名前（Name）」です。
カテゴリの名前とタイプ	カテゴリ名またはカテゴリ タイプを選択します。デフォルト値は「すべて（All）」です。
Grade	[良好（Good）]、[許容（Acceptable）]、[低品質（Poor）]、[すべて（All）]または[該当なし（N/A）]を選択します。デフォルト値は「すべて（All）」です。
Jitter	[ジッター（Jitter）] から範囲を選択して、値をミリ秒単位で入力します。デフォルトの範囲は0以上です。
Packet Loss	[パケット損失] から範囲を選択して、このフィールドに値を入力します。デフォルトの範囲は0以上です。
フレーム損失発生秒数（Conceal Seconds）	範囲を選択し、[秒（seconds）] フィールドに値を入力します。デフォルトの範囲は0以上です。
Conceal Ratio	[フレーム損失率（Conceal Ratio）] から範囲を選択して、このフィールドに値を入力します。デフォルトの範囲は0以上です。

フィールド	説明
Call Type	[音声（Audio）]、[ビデオ（Video）]、または [任意（Any）] を選択します。デフォルト値は「すべて（Any）」です。
Call Class	[オンネット（On Net）]、[オフネット（Off-Net）]、または [任意（Any）] を選択します。デフォルト値は「すべて（Any）」です。
Call Duration	[通話時間（Call Duration）] から通話時間の値を選択し、[秒（secs）] フィールドに時間を入力します。デフォルト値は「すべて（Any）」です。
Termination Type	[成功（Success）]、[失敗（Failed）]、または [任意（Any）] のいずれかを選択します。デフォルト値は「すべて（Any）」です。
Termination Cause Code	[コール終了原因コード（Termination Cause Code）] から原因コードを選択します。デフォルト値は「すべて（All）」です。

フィールド	説明
Time Period	[コール接続時刻（Call Connect Time）] または [コール切断時刻（Call Disconnect Time）]。デフォルト値は [コール接続時刻（Call Connect Time）] です。トップ N のダッシュレットを使用した相互起動の場合、デフォルト値は [コール切断時刻（Call Disconnect Time）] です。 [コール接続時刻（Call Connect Time）]：コールが発信された時間。 [コール切断時刻（Call Disconnect Time）]：通話が終了するまでの時間。 [過去（Past）] を選択するか、開始時刻と終了時刻を入力します。デフォルト値は [過去（Past）] です。 開始時刻のデフォルト値は、現在の時刻の1時間前、終了時刻は現在の時間です。 [過去（Past）] は、分、時間、または日単位で選択できます。[過去（Past）] のデフォルト値は 1 時間です。 たとえば、今日の午後 10 時に 過去 8 時間 を選択した場合、午後 2 時から 9 時 59 分までのレコードが表示されます。 今日 10 時 に過去 1 日を選択した場合は、前日の 午前 12 時から 午後 11 時 59 分までのレコードが表示されます。

[ジッター（Jitter）]、[パケット損失（Packet Loss）]、[フレーム損失発生秒数（Conceal Seconds）]、[フレーム損失率（Conceal Ratio）] フィールドは CMR フィルタのみに適用され、[コールカテゴリ（Call Category）]、[コールタイプ（Call Type）]、[コールクラス（Call Class）]、[通話時間（Call Duration）]、[終了タイプ（Termination Type）]、および[終了原因コード（Termination Cause Code）] フィールド は CDR フィルタのみに適用されます。

ステップ 3 [フィルタを適用（Apply Filter）] をクリックします。

CDR & CMR レポートが生成されます。

選択したフィルタでレコードが使用不可の場合は、利用可能なデータは表示されません。

CDR & CMR レポートには、過去 7 日間のレコードのみが表示されます。

トラブルシュート

1. **問題**：CDR & amp; CMR レポートに、「N/A」としてグレードが表示される。

   推奨処置：Severely Conceal Seconds Ratio 値をエンドポイントから受信していないかどうか、または CMR が存在しないかどうかを確認します。

2. **問題**：Severely Conceal Seconds Ratio が x% であり、コールのグレードは Poor Call だが、実際にはコールの品質は低くない。

   推奨処置：[CDR分析の設定（CDR Analysis Settings）] の [音声通話グレード（Voice Call Grade）] ページで、Severely Conceal Seconds Ratio のしきい値を設定できます。

3. **問題**：コールのグレードが正しくない。

   推奨処置：Severely Conceal Seconds Ratio のしきい値を、コールの CMR レポートの Severely Conceal Seconds Ratio 値に対してクロスチェックします。

4. **問題**：CDR/CMR レコードが受信されない。

   推奨処置：次のいずれかを実行します。

   - PCA を課金サーバとして Unified CM に（追加されていない場合は）追加します。

     PCA を課金サーバとして追加する場合は、CDR の送信がエラーになるのを防ぐために、Unified CM で [障害時に再送（Resend on Failure）] オプションをオンにしてください。

   - Cisco Prime Collaboration Assurance と Unified CM の課金サーバで、SFTP のユーザ名およびパスワードが同じであるかどうかを確認します。
   - Unified CM でCDR Repository Manager または CDR エージェント サービスが稼働しているかどうかを確認します。
   - Unified CM で [CDR有効フラグ（CDR Enabled Flag）] と [コール診断有効（Call Diagnostics Enabled）] のオプションが正しく設定されているかどうかを確認します。
   - ファイアウォールの設定によってファイル転送がブロックされていないかを確認し、ブロックされている場合は、ネットワーク インフラストラクチャ レベルで修正します。
   - クラスタのデータ収集が [通話品質データソース管理（Call Quality Data Source Management）] ページで [失敗（Failed）] 状態である場合は、そのパブリッシャに対して再検出を実行します。Cisco Prime Collaboration Assurance のデバイスのセットアップ、およびデバイス設定のリストに関しては、次のリンク先を参照してください。
     - Cisco Prime Collaboration Assurance のデバイス設定
     - Cisco Prime Collaboration Assurance のデバイス設定

NAM & Sensor Report

NAM & Sensor レポートには、データ、MOS、ジッタ、タイムスタンプを収集したセンサの名前が表示されます。

（注） このレポートは、Cisco Prime Collaboration Assurance を MSP モードでインストールした場合には適用されません。

NAM & Sensor レポートを生成するには、**[アシュアランス レポート（Assurance Reports）]** > **[NAM および センサー レポート（NAM & Sensor Reports）]**。必須フィールドに値を入力し、**[レポートの生成（Report Report）]** をクリックします。

Cisco Prime Collaboration リリース 11.5 以降の場合

選択 **[レポート（Report）]** > **[NAM およびセンサー レポート（NAM & Sensor Reports）]**。

次の表は、NAM & Sensor レポートのフィールドについての説明です。

フィールド	説明
Name	データを収集し、MOS を分析したセンサの内容を示す名前です。 （注） Cisco 1040 と < *MAC* アドレスの下 *6* 桁の番号 > は、Cisco Prime Collaboration Assurance に自動的に登録された Cisco 1040 を識別します。
ID	1040 MAC アドレス、あるいは Cisco Prime Network Analysis Module（Prime NAM）、または Cisco Prime Virtual Network Analysis Module（Prime vNAM）の IP アドレスです。

スピーカー/リスナー	ディレクトリ番号：次のようにデバイスがUnified Communications Managerによって管理されている場合に表示されます。 • 適切なクレデンシャルでvCisco Prime Collaboration Assuranceに追加されます。 • 監視は中断されていません。 デバイスタイプ：デバイスタイプまたは次のいずれかが表示されます。 • N/A：何らかのエラーにより、Cisco Prime Collaboration Assuranceはデバイス タイプを取得できません。 • 利用不可：Cisco Prime Collaboration Assuranceはこの電話を初めて認識し、デバイス タイプがまだ認識されていないか、対応するUnified CMが以下のとおりとなっています。 • Cisco Prime Collaboration Assuranceに追加されていません。 • Cisco Prime Collaboration Assuranceに有効なデバイス タイプが提供されていません。 IPアドレス：IPアドレスがクリックできる場合は、これをクリックして[詳細なデバイス ビュー（Detailed Device View）]ページまたは[電話の詳細（Phone Detail）]ウィンドウを起動します。 UDPポート：メディアストリームのソースであるトランスポート レイヤ ポートです。 Device Name。
時刻	センサーがMOSを計算した時刻。
TOS	サービスのタイプ（TOS）。

MOS	サンプル期間中の平均MOS値。サンプル期間が非常に短い場合、この値はN/Aと表示されるか、または表示されません。 MOSはリスナー側の音質を反映します。値をクリックすると、[Sensor Stream Correlation]ウィンドウが表示されます。
Minimum MOS	サンプル期間中の最小MOSスコア。 サンプル期間が非常に短い場合、この値はN/Aと表示されるか、または表示されません。
Primary Degradation Cause	次のいずれかです。 • ジッタ • パケット損失 • [None]：ジッタとパケット損失の両方の値が0（ゼロ）。 サンプル期間が非常に短い場合、この値はN/Aと表示されるか、または表示されません。
Grade	音声コールのグレード設定に基づきます。次のいずれかを選択します。 • [良好（Good）]：コール値がロングコールのSCSR（%）またはショートコールのSCSR（%）のしきい値を下回っています。 • [可（Acceptable）]：コール値がロングコールSCSR（%）またはショートコールのSCSR (%) のしきい値以上です。 • [不良（Poor）]：コール値がロングコールのSCSR（%）またはショートコールのSCSR（%）のしきい値を上回っています。 • [該当なし（N/A）]：SCSR（%）値が使用できないか、マイナス値です。 • [すべて（All）]：すべてのグレードを選択します。 詳細については、音声通話グレード設定の概要 （276 ページ）を参照してください。

Jitter (ms)	サンプル期間中のジッタ値（ミリ秒単位）。
Packet Loss	サンプル期間中にネットワーク伝送が原因で失われたパケットの数です。観察された RTP シーケンス番号の分析に基づいて計算されます。
Sample Duration(s)	分析対象の最初のパケットから最後のパケットまでの秒数です。この値は通常 60 ですが、最初のストリームまたは最後のストリームの場合は、より小さい値になる可能性があります。
Max Jitter (ms)	サンプル期間中の最大ジッタ値（ミリ秒単位）です。
Adjusted Packet Loss(%)	高ジッタが原因で損失したパケットのパーセンテージ。固定長遅延の参照ジッタ バッファに基づいて計算されます。この値はネットワーク損失の影響は受けません。
パケット損失（%）	パケット損失のパーセントです。（パケット損失を予測される合計パケットで割り、パーセントで表現）。
SSRC	同期ソース ID - RTP パケット ストリームの発信元を識別します。
リスナー DN/IP	MOS と障害の詳細が報告されたエンドポイント（着信側または発信側）を識別します。次のいずれかを示します。 • リスナーの IP アドレスです。 • リスナーの電話番号です。
クラスタ	Unified Communications Manager クラスタです。

発信者/着信者	• **ディレクトリ番号**：コールが行われたディレクトリ番号です。 • **デバイス タイプ**：コールを発信したデバイスのタイプです。 • **シグナリング IP**：コール シグナリングを発信したデバイスの IP アドレスです。IP Phone の場合、このフィールドでは電話機のアドレスが指定されます。PSTN コールの場合、このフィールドでは H.323 ゲートウェイのアドレスが指定されます。 • **B チャネル**：MGCP ゲートウェイの B チャネル番号で、適用されない場合は NA となります。 • **メディア IP**：コールの発信元の IP アドレスです。 • **メディア ポート**：コールの発信元のポートです。 • **デバイス プール**：コールの発信元のデバイス プールです。 • **場所**：コールの発信場所です。
時間範囲の選択	コールを開始した日付と時刻が、Cisco Prime Collaboration Assurance サーバのローカル タイム ゾーン（Unified CM が配置されているタイム ゾーンではなく）で表されています。最大時間の制限は 7 日間です。
Call Duration(s)	コールの長さ（秒単位）。

Impairment Details	• **ジッタ（ms）**：コール中のジッタ（ミリ秒）です。 • **パケット損失**：コール中に失ったパケット数です。 • **隠蔽の秒数**：音声ストリームの開始からの隠蔽イベント（フレームの損失）のあった秒数（深刻な隠蔽の秒数を含む）です。 • **深刻な隠蔽の秒数**：かなりの量の隠蔽（50 ミリ秒を超過）が観察された秒数です。 • **レイテンシ**：遅延 • **隠蔽率**：総フレームに対する隠蔽フレームの割合です。
Call Release Code	• **Caller Termination Cause**：発信者のエンドポイントでコールが終了した理由を表す文字列です。 • **Called Termination Cause**：コールしたエンドポイントでコールが終了した理由を表す文字列です。失敗したコールの原因コードについては、『Cisco Unified Communications Manager コール詳細レコード アドミニストレーション ガイド』の「Call Termination Cause」セクションを参照してください。
Call Category Names	コールが属するカテゴリのカンマ区切りのリスト。詳細については、コール分類（477 ページ）およびコール カテゴリの作成 （480 ページ）を参照してください。
Call Category Types	コール カテゴリが属するカテゴリ タイプのカンマ区切りのリスト。詳細については、コール分類 （477 ページ）およびコール カテゴリの作成 （480 ページ）を参照してください。

Call Class	次のいずれかです。 • Offnet • Onnet **注** 詳細については、OffNet および OnNetNet コールを理解する （480 ページ） を参照してください。
Severely Conceal Seconds Ratio (%)	音声品質を測定するメトリック。深刻な隠蔽の秒数（SCS）と時間の比率です。
Conceal Seconds Ratio (%)	ネットワーク品質を測定するメトリック。隠蔽の秒数（CS）と時間の比率です。

NAM & Sensor レポートは CSV 形式でエクスポートできます。

レポートをエクスポートするには、レポート ウィンドウの右側のペインにある **[エクスポート（Export）]** ツールボタンをクリックします。**[すべて（ALL）]** を選択するか、**[範囲（Range）]** ラジオ ボタンに値を入力し、**[OK]** をクリックします。ファイルをエクスポートしようとしたときにクライアントシステムが応答しない場合は、ファイルのダウンロードに関する問題のトラブルシューティングを参照してください。

センサー レポートを理解する

2 つの RTP ストリーム（着信および発信）で 1 つの音声コールを構成します。センサーは次のようなさまざまな方法で音声トラフィックをキャプチャします。

- Cisco 1040 は、音声トラフィックをミラーリングするように設定されたスイッチポートアナライザ（SPAN）ポートで RTP 音声トラフィックを受信します。Cisco 1040 は、電話機ポートと SPAN ポートがミラーする音声 VLAN に応じて、1 つまたは両方の RTP ストリームのみをリッスンして MOS を計算し、データを 60 秒間隔で Cisco Prime Collaboration Assurance に送信します。
- Cisco Prime Network Analysis Module（Prime NAM）または Cisco Prime Virtual Network Analysis Module（Prime vNAM）も、SPAN ポートからデータをキャプチャできます。また、Cisco Prime Network Analysis Module（Prime NAM）または Cisco Prime Virtual Network Analysis Module（Prime vNAM）を設定し、データをキャプチャする他の方法として使用することもできます。Cisco Prime Collaboration Assurance が必要なデータを Cisco Prime Network Analysis Module（Prime NAM）または Cisco Prime Virtual Network Analysis Module（Prime vNAM）が提供するには、Cisco Prime Network Analysis Module（Prime NAM）または Cisco Prime Virtual Network Analysis Module（Prime vNAM）で RTP ストリームの監視を有効にする必要があります。Cisco Prime Collaboration Assurance は、Cisco Prime Network Analysis Module（Prime NAM）または Cisco Prime Virtual Network Analysis Module（Prime vNAM）から 60 秒間隔でデータを取得します。

センサー レポートには、RTP ストリームについてセンサーが 1 分ごとに計算した MOS を表示します。センサー レポートには、一方だけまたは両方の RTP ストリームがキャプチャされたかどうかに応じて、1 分ごとに 1 行または 2 行のデータが表示されます。各行に、データを収集したセンサー、関係するエンドポイント、MOS、ジッタ（ミリ秒単位）、およびタイム スタンプが示されます。

センサー ストリーム相関データの表示

[センサー ストリーム相関関係（Sensor Stream Correlation）] ウィンドウを起動するには、センサーレポートを生成し、対象とするストリームの グレード値をクリックします。

（注） [センサー ストリーム相関関係（Sensor Stream Correlation）] ページの代わりに 「[サーバが見つかりません]（Cannot find server）」 ページが表示された場合は、センサー ストリーム相関関係ウィンドウの表示を参照してください。

Cisco Prime Collaboration Assurance は、センサーからのデータを相互に関連付けて、Unified CM コール レコードと比較し、次の情報が記載された表を表示します。

- ストリームの概要：センサーレポートに表示されたデータのサブセットです。ストリームの同期ソース（SSRC）ID も表示されます。SSRC は RTP パケット ストリームの発信元を識別し、RTP 会議中は一意のままになります。

  （注） リスナー エンドポイントと UDP ポートが RTP パケットのストリームのソースである場合、別の SSRC が送信された RTP ストリームにも割り当てられます。[Sensor Stream Correlation] ウィンドウは、1 つの SSRC のデータのみを相関分析します。

- コール レコード：ストリームに関連付けられた Unified CM CDR からの情報です。

  （注） コールがまだ終了していない場合は、表の見出しに「No Call Detail Record found for these streams」と表示されます。

- [Stream details]：SSRC がストリーム サマリー内のセンサーと一致している 1 つ以上のセンサーの詳細。

次の表には、ストリームの概要テーブルに表示されたデータが示されています。

表 *63 : Stream Summary*

列	説明

スピーカー/リスナー	• ディレクトリ番号：次のようにデバイスが Unified Communications Manager によって管理されている場合に表示されます。 • 適切なクレデンシャルで vCisco Prime Collaboration Assurance に追加されます。 • 監視は中断されていません。 • IP アドレス：デバイス タイプに応じて、[IP フォンの詳細（IP Phone Details）] ページまたは [詳細なデバイス ビュー（Detailed Device View）] が開きます。 • UDP ポート：メディア ストリームのソースであるトランスポート レイヤ ポートです。 • デバイス タイプ：デバイス タイプまたは次のいずれかが表示されます。 • N/A：何らかのエラーにより、Cisco Prime Collaboration Assurance はデバイス タイプを取得できません。 • 利用不可：Cisco Prime Collaboration Assurance はこの電話機を初めて認識し、デバイス タイプがまだ認識されていないか、対応する Unified CM が次のとおりとなっています。 • Cisco Prime Collaboration Assurance に追加されていません。 • Cisco Prime Collaboration Assurance に有効なデバイス タイプが提供されていません。
TOS	サービスのタイプ。
コーデック	コーデック名。
SSRC	同期ソース ID：RTP パケット ストリームの発信元を識別します。

次の表には、使用できる場合に CDR からのデータが示されています。コールがまだ終了していない場合は、表の見出しに「No Call Detail Record found for these streams」と表示され、行は空白になります。

表 *64 : Call Record*

列	説明
Call Disconnect	コールが切断された時刻。コールが切断されていない場合、ゼロ（0）が表示されます。
Cluster ID	Unified CM クラスタ ID です。
Caller Signaling IP	コール シグナリングを発信したデバイスの IP アドレス。Cisco Unified IP 電話 の場合、このフィールドでは電話機のアドレスが指定されます。PSTN コールの場合、このフィールドでは H.323 ゲートウェイのアドレスが指定されます。
Caller B-Channel	MGCP ゲートウェイの B チャネル番号。適用されない場合は NA。
Called Signaling IP	コール シグナリングを終端したデバイスの IP アドレス。
Called B-Channel	MGCP ゲートウェイの B チャネル番号。適用されない場合は NA。
Call Duration (s)	コールの長さ（秒単位）。
Caller Termination Cause	発信側がコールを解放したときに表示されます。 （注） 終了した理由は表示されない場合があります。
Called Termination Cause	終端側がコールを解放したとき、またはコールが拒否されたときに表示されます。 （注） 終了した理由は表示されない場合があります。

次の表には、ストリームの概要テーブルと一致する SSRC でストリームからのデータが示されています。

表 *65 :* ストリームの詳細

列	説明

センサー名	Cisco 1040、Cisco Prime Network Analysis Module（Prime NAM）、または Cisco Prime Virtual Network Analysis Module（Prime vNAM）の表示名です。
時刻	センサーが MOS を計算した時刻。
MOS	サンプル期間中の平均 MOS 値。
Minimum MOS	サンプル期間中の最小 MOS 値。
Primary Degradation Cause	Jitter、Packet Loss、または None（ジッタとパケット損失の値がどちらもゼロ（0）の場合）。
Jitter (ms)	ジッタ値（ミリ秒単位）。
Packet Loss	パケット損失数。（サンプル期間中に失われた実際のパケット数）。
Sample Duration (s)	分析対象の最初のパケットから最後のパケットまでに経過した秒数。
Max Jitter (ms)	最大のジッタ値（ミリ秒単位）。
Adjusted Packet Loss (%)	高ジッタが原因で損失したパケットのパーセンテージ。固定長遅延の参照ジッタ バッファに基づいて計算されます。この値はネットワーク損失の影響は受けません。
パケット損失（%）	パケット損失のパーセンテージ。（実際のパケット損失を予測される合計パケットで割り、パーセントで表現）。

センサー ストリーム相関関係ウィンドウの表示

[センサー ストリーム相関関係（Sensor Stream Correlation）] ウィンドウを開こうとしたときに「「ページが見つかりません」」などのメッセージが表示された場合、この問題は、ブラウザのプロキシ サーバ設定を無効にすることで解決できます。この設定は、[接続（Connection）] タブの [インターネット オプション（Internet Options）] にあります。

セッション レポート/会議レポート

会議レポートを使用して、すべての会議の概要レポートや会議の詳細レポートを表示できます。

Cisco Prime Collaboration リリース 12.1 SP2 以降の場合

会議レポートの前提条件

会議レポートには、次の要件があります。

- Unified CM および Cisco VCS は、Managed 状態にある必要があります。
- MCU などのエンドポイントとコントローラは、Managed 状態にある必要があります。
- デバイスの可視性を 「Full Visibility」 状態に設定します。
- JTAPI が Unified Communications Manager で設定されている必要があります。Unified Communications Manager で JTAPI を有効にする方法については、「Cisco Prime Collaboration Assurance のデバイス設定」を参照してください。
- Cisco Prime Collaboration Assurance サーバが、Cisco VCS でフィードバック サーバとして登録されている必要があります。
- 会議の診断と音声電話機能の模擬テストを正しく実行するには、Cisco Prime Collaboration Assurance Service Pack 1 バンドルを適用する前に、CUCM がリストされているバージョンであることを確認してください。詳細については、12.1 Service Pack 1 の『Cisco Prime Collaboration Assurance でサポートされているデバイス』を参照してください。

次の会議レポートを生成できます。

すべてのセッション/会議の要約レポート

会議の要約レポートは、進行中および完了した会議に関する情報を提供します。レポートは 4 週間保持されます。

このレポートには、エンドポイント名、デバイス ID、合計使用率、平均継続期間、および最長の会議が含まれます。

また、スケジュールされている会議のスケジュール期間が表示されます。この値は、アドホック会議では「NA」と表示されます。さらに、スケジュールされた時間の使用率もパーセンテージで表示されます。

次の情報も確認できます。

- [IPアドレス（IP address）]：会議に参加した、選択されたエンドポイントの IP アドレスを表示します。
- [プロトコル（Protocol）]：会議に使用されたプロトコルを表示します。これは、[エンドポイント（Endpoint）] ペインの [参加した会議（Participated conferences）] に表示されます。

以下の詳細を確認するには、電話機の可視性が [完全（Full）] に設定されている必要があります。

次の情報も確認できます。

- [受信したビデオDSCP（Received Video DSCP）]：会議で最後に受信したビデオ デバイスの DSCP 値。これは、Cisco Unified IP 電話 8941 と 8945、Cisco DX シリーズ、および Cisco TelePresence TX シリーズにのみ適用されます。
- [受信したオーディオDSCP（Received Audio DSCP）]：会議で最後に受信したオーディオ デバイスの DSCP 値。これは、Cisco Unified IP 電話 8941 と 8945、Cisco DX シリーズ、および Cisco TelePresence TX シリーズにのみ適用されます。
- [パケット損失のピーク（Peak Packet Loss）]：会議で発生したパケット損失の最高値（パーセンテージ）。

すべてのセッションの 要約レポートを生成するには、**[アシュアランスレポート（Assurance Reports）]** > **[セッションレポート（Session Reports）]** > **[すべてのセッションの要約レポート（All Session Summary Report）]** 。

Cisco Prime Collaboration リリース 11.5 以降の場合

移行方法 **[レポート（Reports）]** > **[会議レポート（Conference Reports）]** > **[会議の概要レポート（Conference Summary Report）]**。

Session/Conference Detail レポート

会議詳細レポートには、会議 ID、時間、開始/終了時間、会議のタイプ、ステータス、アラームの重大度などの詳細情報が表示されます。

会議の詳細 レポートを生成するには、 を選択します。**[アシュアランスレポート（Assurance Reports）]** > **[セッション レポート（Session Reports）]** > **[セッション詳細レポート（Session Detail Report）]**。

Cisco Prime Collaboration リリース 11.5 以降の場合

移行方法 **[レポート（Reports）]** > **[会議レポート（Conference Reports）]** > **[会議の詳細レポート（Conference Detail Report）]**。

TelePresence エンドポイント レポート

TelePresence レポートを使用すると、エンドポイントの使用率、不参加エンドポイント サマリーを表示できます。

Cisco Prime Collaboration リリース 12.1 SP2 以降の場合

Telepresence エンドポイント レポートの前提条件

Telepresence エンドポイント レポートには、次のものが必要です。

- Unified CM および Cisco VCS は、Managed 状態にある必要があります。
- MCU などのエンドポイントとコントローラは、Managed 状態にある必要があります。
- デバイスの可視性を 「Full Visibility」 状態に設定します。

- JTAPI が Unified Communications Manager で設定されている必要があります。Unified Communications Manager で JTAPI を有効にする方法については、「Cisco Prime Collaboration Assurance のデバイス設定」を参照してください。
- Cisco Prime Collaboration Assurance サーバが、Cisco VCS でフィードバック サーバとして登録されている必要があります。
- 会議の診断と音声電話機能の模擬テストを正しく実行するには、Cisco Prime Collaboration Assurance Service Pack 1 バンドルを適用する前に、CUCM がリストされているバージョンであることを確認してください。詳細については、12.1 Service Pack 1 の『Cisco Prime Collaboration Assurance でサポートされているデバイス』を参照してください。

次のレポートは、TelePresence エンドポイントに対して生成できます。

Endpoint Utilization Report

Endpoint Utilization レポートにより、最も使用率の高いエンドポイントおよび最も使用率の低いエンドポイントを識別できます。

エンドポイントの平均使用率は、次の式を使用して計算されます。

- システム定義（1 日、1 週間、4 週間）レポート：

  （合計使用時間（分）/[最大使用時間 *60]）* 100

- カスタム レポートの場合：

  （合計使用時間（分）/（[最大使用時間 * 60 * 日数]））* 100

  - 1 日：最大使用時間は 10 時間です。
  - 1 週間：最大使用時間は 50 時間です。
  - 4 週間：最大使用時間は 200 時間です。
  - カスタム レポート：最大使用時間は 1 日あたり 7.14 時間です。

スケジュールされた時間の使用率を % で示し、これは、スケジュールされた時間の使用状況をパーセンテージで表しています。

エンドポイントの使用率の設定はカスタマイズできます。カスタマイズするには、エンドポイントモデル（特定のモデルのエンドポイント）を選択して、[使用率の変更（Change Utilization）] ボタンをクリックします。1 日の作業時間数と 1 週間の作業日数を選択できます。

エンドポイント使用率レポートを生成するには、**[アシュアランス レポート（Assurance Reports）]** > **[Telepresence エンドポイント レポート（Telepresence Endpoint Reports）]** > **[エンドポイント使用率レポート（Endpoints Utilization Report）]**。

Cisco Prime Collaboration リリース 11.5 以降の場合

移行方法 **[レポート（Reports）]** > **[Telepresence エンドポイントレポート（Telepresence Endpoint Reports）]** > **[エンドポイント使用率レポート（Endpoint Utilization Report）]**。

No Show エンドポイントの要約レポート

No Show Endpoints Summary レポートには、スケジュールされた会議に参加しなかったエンドポイントに関する情報が表示されます。このレポートは、スケジュールされて完了した会議データに基づき生成されます。

エンドポイント表示なしサマリー レポートを生成するには、次のオプションを選択します。**[アシュアランス レポート（Assurance Report）] > [Telepresence レポート（Telepresence Report）] > [エンドポイント使用率レポート（Endpoint Utilization Report）]**。

Cisco Prime Collaboration リリース 11.5 以降の場合

エンドポイント表示なしサマリー レポートを生成するには、次のオプションを選択します。**[レポート（Report）] > [Telepresence エンドポイント レポート（Telepresence Endpoint Reports）] > [No Show エンドポイントの要約レポート（No Show Endpoint Summary Report）]**。

[CUCMレポートの起動（Launch CUCM Reports）]

[CUCMレポートの起動（Launch CUCM Reports）] では、Cisco Unified Communications Manager クラスタのレポート ページをクロス起動できます。

次に進む: **[CUCMレポートの起動（Launch CUCM Reports）]**をクリックして、クラスタ名をクリックして Cisco Unified Reporting アプリケーションを開きます。

Cisco Prime Collaboration リリース 11.5 以降の場合

選択 **[レポート（Reports）] > [CUCMレポートの起動（Launch CUCM Reports）]**。

その他のレポート

その他のレポート、UCM/CME Phone Activity レポート、Voice Call Quality Event History レポートなど、さまざまなレポートを使用できます。

UCM/CME Phone Activity Reports

UCM/CME Phone Activity レポートは、過去 30 日間にステータス変更のあった、オーディオおよびビデオ電話に関する情報を提供します。

Cisco Prime Collaboration Assurance を Enterprise モードで導入した場合、Export Audio Phones レポートを除く Phone Activity レポートには、ドメイン名が表示されます。

Cisco Prime Collaboration Assurance を MSP モードで導入した場合、Export Audio Phones レポートを除く Phone Activity レポートには、顧客名が表示されます。

利用可能な Activity レポートは、次のとおりです。

Endpoint Move レポート

[Endpoint Move] レポートには、過去 30 日以内に移動された IP/ビデオ エンドポイントの詳細が表示されます。また、移動前後に使用されている内線、Cisco Unified CM アドレス、スイッチのアドレス、スイッチ ポートを表示します。

[Endpoint Move]レポートには、IP/ビデオ エンドポイントの移動が発生した時間ではなく、検出された時間が表示されます。

[Endpoint Move] レポートを生成するには、**[レポート（Reports）]** > **[その他のレポート（Miscellaneous Reports）]** > **[Endpoint Move]** の順に選択します。

（注） **[Endpoint Move]** レポートは、CDP をサポートしないビデオ エンドポイントはサポートしていません。

Endpoint Audit レポート

Endpoint Audit Report には、管理されている IP/ビデオ エンドポイント ネットワーク内の変更が表示されます。

たとえば、このレポートには、ネットワークで追加または削除された IP/ビデオ エンドポイント、IP またはビデオ エンドポイントのステータスなどが表示されます。たとえば、エンドポイントのステータスは、エンドポイントが Cisco Unified CM から登録を解除されたときに変更されます。

Endpoint Audit Report を生成するには、**[レポート（Reports）]** > **[その他のレポート（Miscellaneous Reports）]** > **[UCM/CME Phone Activity Reports]** > **[エンドポイントの監査（Endpoint Audit）]** の順に選択します。

（注） 24 時間以上前に CUCM から登録解除されたエンドポイントは、Audit Report に [Removed（削除済み）] と表示されます。レコードの場合、登録されている間に CUCM から削除されたエンドポイントは、Audit Report に次の 24 時間は [未登録（Unregistered）] と表示され、それ以降は [Removed（削除済み）] と表示されます。これらは、削除後に最初の CDT 検出を行った後には、Cisco Prime Collaboration Assurance インベントリから削除されることに注意してください。

Endpoint Remove レポート

[Endpoint Remove] レポートには、過去 30 日以内に削除されたエンドポイントが一覧表示されます。

[Endpoint Move] レポートを生成するには、**[レポート（Reports）]** > **[その他のレポート（Miscellaneous Reports）]** > **[Endpoint Move Report]** の順に選択します。

Endpoint Extension レポート

Endpoint Extension Report には、過去 30 日以内に内線番号が変更されたエンドポイントが一覧表示されます。

Endpoint Extension Report を生成するには、**[レポート（Reports）] > [その他のレポート（Miscellaneous Reports）] > [Endpoint Extension Report]** の順に選択します。

（注） Endpoint Extension Report は、Cisco ワイヤレス IP 電話 7920 ではサポートされていません。

Audio IP Phone Activity レポートの対象期間を理解する

Cisco Prime Collaboration リリース 11.1 以前の場合

Audio IP Phone レポートまたは Video IP Phone Activity レポートを生成する場合は、次のそれぞれがどの時間帯の地域に属しているかによってレポートの結果が影響を受ける場合があります。

- クライアント システム：Cisco Prime Collaboration Assurance は、クライアント システムの日時に基づき、Phone Activity レポートの期間（レポートに応じて、直近 24 時間から直近 7～30 日まで）を計算します。
- Prime Collaboration システム：Cisco Prime Collaboration Assurance は、内線番号の変更など、Cisco Prime Collaboration システムが検出した変更の時間に基づき、一部の監査を記録します。
- Cisco Unified Communications Manager：Cisco Prime Collaboration Assurance は、電話機の移動など、Cisco Unified CM が検出した変更の時間に基づき、一部の監査を記録します。

これらのシステムに 1 つでも同じ時間帯に属していないものがある場合は、Phone Activity レポートを生成および表示するときに、時間帯の差を考慮に入れる必要があります。

（注） Cisco Prime Collaboration Assurance システムの監査日時と Audio IP Phone または Video IP Phone Audit レポートに表示される監査日時が一致しない場合は、ネットワーク内のすべての Cisco Unified CM が同期するように設定されていることを確認します。

Cisco Unified CM がダウン時に電話機のステータスをトラッキング

Cisco Prime Collaboration リリース 11.1 以前の場合

バックアップが設定済みの Cisco Unified CM がダウンすると、音声やビデオ IP フォンは Cisco Unified CM のバックアップにフェールオーバーします。

Cisco Prime Collaboration Assurance は、バックアップに登録された電話機の監査レコードを保存し、これらの変更されたステータスは IP Phone and Video Phone Audit レポートに含まれます。

Cisco Prime Collaboration Assurance は、次の場合には監査レコードを保存しません。

- Cisco Unified CM クラスタ全体がダウンする。

  バックアップが設定されていない Cisco Unified CM がダウンする。

そのため、このような Cisco Unified CM に登録された電話機のステータスが変更された状況では、Audio IP Phone Status and Video IP Phone Activity レポートには含まれません。

Voice Call Quality Event History Reports

次の項目に基づき、[Voice Call Quality] イベントの [Event History] データベースを検索できます。

- MOS
- 接続先
- コーデック
- 電話機モデル
- センサー（Cisco Prime Collaboration Assurance を MSP モードでインストールした場合には適用されません）
- 日付
- エクスポート

Call Quality Event History レポートを生成するには、**[アシュアランス レポート（Assurance Reports）]** > **[その他のレポート（Miscellaneous Reports）]** > **[音声コールの品質のイベント履歴レポート（Voice Call Quality Event History Reports）]**。

Cisco Prime Collaboration リリース 11.5 以降の場合

移行方法 **[レポート（Reports）]** > **[その他のレポート（Miscellaneous Reports）]** > **[Voice Call Quality Event History レポート（Voice Call Quality Event History Reports）]** 。

Voice Call Quality Event History レポートは、検索基準に基づき最大 2000 件の記録を一覧表示するスクロール可能な表です。

2,000 レコードを超えてデータベースの内容を表示するには、の順に選択します。**[アシュアランス レポート（Assurance Reports）]** > **[その他のレポート（Miscellaneous Reports）]** > **[音声コールの品質のイベント履歴レポート（Voice Call Quality Event History Reports）]** > **[エクスポート（Export）]**。1,000 を超えるレコードが検索基準に一致する場合、ポップアップ ウィンドウに一致するレコードの合計数がレポートされます。

Cisco Prime Collaboration リリース 11.5 以降の場合

選択 **[レポート（Reports）]** > **[その他のレポート（Miscellaneous Reports）]** > **[Voice Call Quality Event History レポート（Voice Call Quality Event History Reports）]** > **[エクスポート（Export）]**。

Internet Explorer ブラウザで Voice Call Quality Event History レポートをエクスポートする場合、**[Windows セキュリティ（Windows Security）]** ポップアップ ウィンドウが表示し、クレデンシャルの入力を要求される場合があります。**[Windows セキュリティ（Windows Security）]** ポップアップ ウィンドウを閉じたとしても、レポートはダウンロードされます。

[Save at（保存先）] フィールドに、Cisco Prime Collaboration Assurance がインストールされているサーバでレポートの保存先を入力します。デフォルトの場所は /opt/emms/cuom/ServiceQualityReports です。

（注） デフォルトの場所にファイルを保存するようにエクスポート設定を構成している場合は、必ず Cisco Prime Collaboration Assurance サーバにログインして、[エクスポート設定（Export Settings）] ページで入力したフォルダーを作成し、ユーザのフォルダに書き込み権限を与えます。これらのタスクを実行しないと、Cisco Prime Collaboration Assurance はエクスポート ファイルを作成できません。

[メール送信先（E-mail to）] フィールドに、1 つまたはコンマで区切られた複数の完全な電子メールアドレスを入力します。

レポートをダウンロードするには、**[レポートのダウンロード（Download Report）]** をクリックします。

Cisco Prime Collaboration Assurance を Enterprise モードで導入した場合は、グローバル セレクタ（ドロップダウン）で選択した特定のドメインの Call Quality Event History レポートのみを表示できます。ただし、エクスポート オプションを使用してレポートをエクスポートした場合、レポートはグローバル セレクタで選択したドメインに基づきフィルタリングされません。

Cisco Prime Collaboration Assurance を MSP モードで導入した場合、Call Quality Event History には名前など、お客様の詳細情報が含まれます。グローバルセレクタ（ドロップダウン）で選択した特定のお客様のレポートを表示できます。ただし、エクスポート オプションを使用してレポートをエクスポートした場合、レポートはグローバル セレクタで選択したお客様に基づきフィルタリングされません。また、このモードでは、センサーに基づいた Voice Call Quality イベントの、イベント履歴データベースを検索することもできません。

その他のレポート

Cisco Prime Collaboration Assurance を Enterprise モードで導入した場合、その他のレポートでは、CTI アプリケーション、Cisco Analog Telephone Adaptor（ATA）デバイス、Cisco 1040 センサーに関する情報を提供します。

（注） Cisco Prime Collaboration Assurance を MSP モードで導入した場合、Cisco 1040 センサーのレポートを生成することはできません。

これらのレポートを生成するには、次のオプションを選択します。**[アシュアランスレポート（Assurance Reports）]** > **[その他のレポート（Miscellaneous Reports）]** > **[その他のレポート（Other Reports）]** をクリックして、レポートを選択します。

Cisco Prime Collaboration リリース 11.5 以降の場合

選択 **[レポート（Reports）]** > **[その他のレポート（Miscellaneous Reports）]** > **[その他のレポート（Other Reports）]**。

CTI Applications レポートの生成

CTI アプリケーション レポートには、Cisco Unified CM に登録されている CTI アプリケーションの一覧が報告されます。

Cisco Unified CM には、次のアプリケーションが CTI デバイスまたは CTI ポートとして登録されます。

- Cisco Personal Assistant
- Cisco Customer Response Applications
- Cisco IP Contact Center
- Cisco Emergency Responder

ATA Devices レポート

ATA Devices レポートは Cisco Unified CM に登録されている ATA デバイスについての情報を提供します。

Cisco 1040 Sensors レポート

Cisco 1040 センサー レポートは、ネットワークに展開された Cisco 1040 センサーに関する情報を提供します。Cisco 1040 センサー レポートを生成する前に、「Cisco Prime Collaboration Assurance レポートを生成するための前提条件」で前提条件を確認してください。

（注） このレポートは、Prime Collaboration を MSP モードでインストールした場合は使用できません。

IP フォンの Web インターフェイスがアクセス可能になっている場合は、次のいずれかのハイパーリンクをクリックすることにより、Cisco 1040 Sensors レポートから Web インターフェイスを開くことができます。

- 内線番号
- MAC アドレス
- IP アドレス

会議デバイスのビデオ ポートの使用率レポート

このレポートは、会議デバイスの 1 時間単位の使用率に基づいて生成されます。

Average Utilization

- 1 日：平均使用率 1 時間目 + 2 時間目 + ... + 24 時間目) / 24。
- 1 週間：1 週間の毎時間の平均使用率を合計し、(7 x 24) で除算します。
- 4 週間：4 週間の毎時間の平均使用率を合計し、(7 x 24 x 4) で除算します。
- カスタム期間：カスタム期間中の毎時間の平均使用率を合計し、(24 x カスタム期間の日数) で除算します。

（注） 使用率は、100% を超えた場合でも 100% と表示されます。

Peak Utilization

- 1 日：24 時間の各時間における個々のピーク値からピーク使用率を分析します。
- 1 週間：7 * 24 時間の各時間における個々のピーク値からピーク使用率を分析します。
- 4 週間：7 * 24 * 4 時間の各時間における個々のピーク値からピーク使用率を分析します。
- カスタム期間：カスタム期間中の各時間における個々のピーク値からピーク使用率を分析します。

会議デバイスの使用率レポートを生成するには、を選択します。**[アシュアランス レポート（Assurance Reports）] > [その他のレポート（Miscellaneous Reports）] > [他のレポート（Other Reports）] > [会議デバイスの使用率レポート（Conferencing Device Utilization Report）]**。

Cisco Prime Collaboration リリース 11.5 以降の場合

移行方法 **[レポート（Reports）] > [その他のレポート（Miscellaneous Reports）] > [その他のレポート（Other Reports）] > [会議デバイスの使用率レポート（Conferencing Device Utilization Report）]** 。

[平均使用率（Average Utilization）] または [ピーク使用率（Peak Utilization）] 列の値をクリックすると、[ビデオポートの使用率の詳細（Detailed Video Port Utilization）] グラフが開きます。表示するデータとして、時間あたりの平均使用率、ピーク使用率、または実際のデータ（[すべて（All）] をクリック）を選択できます。また、スライダを使用して短い時間間隔（1 分間など）を選択して、その時間内の実際のデータを確認することもできます。

スケジュール済みレポート

スケジュール設定されたレポートは、[起動パッドのレポート（Report Launch Pad）] からスケジュールすることができる、使用率およびインベントリに関するレポートです。スケジューリ

ング設定に従ってレポートを生成できます。ダウンロードしたり、設定済みの電子メール ID に送信することができます。これらのレポートは、CSV および PDF 形式にエクスポートできます（ただし、CSV 形式のみでエクスポート可能な Conference Detail レポートは除く）。これらのレポートのデータは、30 日間のみ利用できます。

これらのレポートは、デフォルトでは有効になっていません。レポートは、その場で生成するか、スケジューリングを有効にして事前に定義された日に生成できます。

[レポート（Reports）] -> **[スケジュール済みレポート（Scheduled Reports）]** -> **[レポート（Reports）]** の順にクリックします。

次のスケジュール済みレポートを使用できます。

レポート タイトル	説明
Utilization Report（[レポート（Report）] セレクタで [使用率（Utilization）] > [エンドポイント（Endpoint）]、[エンドポイントの非表示（Endpoint No Show）] の順に選択すると、Monthly Utilization および Monthly No Show Report が表示されます。	
Monthly Utilization Report	エンドポイントの使用率について、月ごとに集計したレポートです。この集計値は、すべての月の使用率 / 12 によって計算されます。
Monthly No Show Report	スケジュール設定された会議には参加していないエンドポイントの、集計された月次レポートを提供します。平均の集計値は、すべての月にわたる不参加割合の合計/12 として計算されます。
Conference Detail レポート	すべての完了した会議で、会議の詳細統計を提供します。
Inventory Report	
Managed Devices Report	管理されたデバイスに関する情報を提供します。不明なデバイスの場合は、IP アドレスのみが表示されます。このレポートを使用して、クレデンシャルが更新されたデバイスを検索します。
Unmanaged Devices Report	管理されていないデバイスに関する情報を提供します。このレポートを使用して、クレデンシャルの更新が必要なデバイスを特定します。

レポート タイトル	説明
エンドポイント	[エンドポイントの診断（Endpoints Diagnostic）] ページで表示されるとおり、エンドポイントに関する情報を提供します。詳細については、エンドポイントの診断ダッシュボード（302ページ）セクションを参照してください。 （注） Cisco Unified Communications Manager（Call Manager）の説明は、Endpoint Report のエンドポイント名列にマップされます。 **[エンドポイント名（Endpoint Name）]**と**[ユーザ名（User Name）]**列の関連付けは、Cisco Jabber または Client Services Framework（CSF）の一意なデバイスの識別に役立ちます。
Cisco Prime Collaboration リリース 12.1 SP3 以降の場合 Endpoint(s) Report（[レポート（Report）] セレクタで **[インベントリ（Inventory）]** -> **[エンドポイント（Endpoint）]** の順にクリック）には、Endpoints Audit、Endpoints Move、Endpoints Remove、Endpoints Extension Audit のスケジュール済みレポートが表示されます。	
	Cisco Prime Collaboration リリース 12.1 SP3 以降の場合 Endpoints Audit、Endpoints Move、Endpoints Remove、Endpoints Extension Audit レポートをスケジュール設定し、生成されたレポートを、電子メール通知経由で指定の電子メール ID に送信できます。生成されたレポートには、過去 1 日の詳細が一覧化されている必要があります。 Cisco Prime Collaboration Assurance を MSP モードで導入した場合、**[顧客（Customer）]** 名の列があります。
Event History Report	
すべてのイベント	過去 1 日、1 週間、1 か月の間に発生したすべてのイベント履歴が提供されます。

（注） Scheduled Utilization レポート（Monthly Utilization、Monthly No Show、Conference Detail レポート）は、ビデオ電話機と TelePresence ポイントに適用できます。これらのレポートに示されるエンドポイントの詳細は、購入したライセンスに基づいて設定されます。

スケジュールされたレポートの生成

目的に応じて、レポート期間、レポート生成日と生成頻度を定義できます。

スケジュール レポートを生成するには、次の手順を実行します。

ステップ 1 [レポート（Reports）] ペインからレポートを選択します。

ステップ 2 [Report Details] ペインの下にある [Settings] タブをクリックし、[Enable Scheduling] をクリックします。

ステップ 3 [Scheduler] および [Settings] ペインのオプションを使用して、レポート生成をスケジューリングします。

ステップ 4 次のいずれかを実行します。

- **[保存（Save）]** をクリックします。
- その場でレポートを生成するには、次の手順を実行します。
  - 生成するレポートの横の [今すぐ実行（Run Now）] をクリックします。
  - [Report Details] ペインで [Run History] タブをクリックします。
  - レポートをダウンロードします。

カスタマイズされ、スケジュールされたレポートを作成するには、左の隅にあるレポートのクイック表示からレポートを選択し、[レポート（Reports）]ペインの下にある [新規（New）] をクリックします。必要な情報を入力し、[Submit] をクリックします。実行レポートのインスタンスは、[Job Management] ページの下のジョブとしてキューに格納されます。これらのジョブの管理とモニタリングは、[管理（Administration）] ページ（から可能です。**[システム管理（System Administration）] > [ジョブ管理（Job Management）]**。

2,000件を超えるレコードを含むレポートのデータへのアクセス

Cisco Prime Collaboration Assurance のレポートには、最大 2,000 件のレコードが表示されます。レポートの生成時に 2,000 件を超えるレコードが返された場合、Cisco Prime Collaboration Assurance は、レポートの表示前に情報メッセージを表示します。

この場合、次のように対処できます。

- フィルタの詳細な条件を指定し、生成されるレポートのレコード数を減らす。
- レポート データを CSV ファイルにエクスポートして、追加のレコードにアクセスする。エクスポート ウィンドウを開くには、レポート ウィンドウの右上隅にある [Export] アイコンをクリックします。CSV ファイルに最大 30,000 レコードをエクスポートできます。

（注） ファイルをエクスポートしようとしたときにクライアントシステムが応答しない場合は、「ファイルのダウンロードに関する問題のトラブルシューティング」を参照してください。

ファイルのダウンロードに関する問題のトラブルシューティング

Cisco Prime Collaboration Assurance からレポートまたは他のデータをファイルにエクスポートしようとしたときに、[エクスポート（export）] ダイアログボックスまたはエクスポート ファイルを保存するよう指示するウィンドウが表示されない場合は、次の手順を使用して問題を解決します。

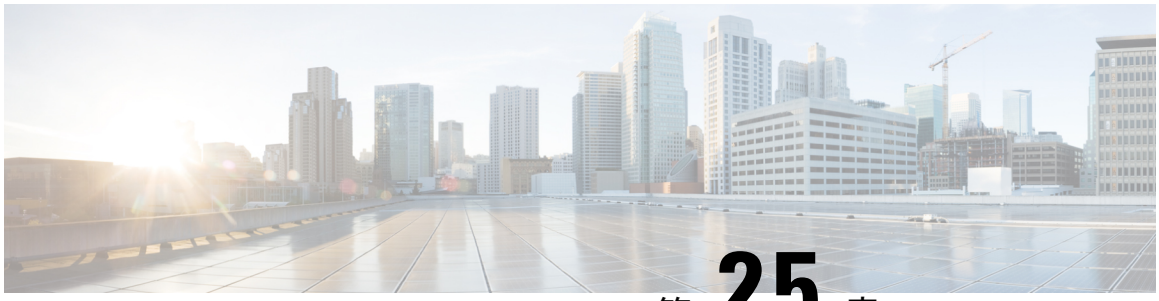
手順

	コマンドまたはアクション	目的
ステップ 1	Internet Explorer でセキュリティのレベルを中以上に設定すると、ファイルのダウンロード時に自動的にダイアログを表示するオプションが無効に設定されます。PDF または CSV ファイルをクライアント システムにダウンロードしようとしたときに、そのシステムに Adobe Acrobat Reader や Microsoft Excel がインストールされていない場合は、何も起きません。その PDF ファイルまたはスプレッドシートは表示されず、ファイルの保存場所を指定するウィンドウも表示されません。ファイルのダウンロードウィンドウを表示できるようにするには、デスクトップで次の手順を実行します。	
ステップ 2	Internet Explorer を使用しており、ファイルのダウンロード時に自動的にダイアログを表示するオプションが有効にされていても、ファイルの保存場所を指定するウィンドウが表示されない場合は、次の手順を実行してください。	

第 VII 部

ネットワークの分析

• Analytics のダッシュボードとレポート （537 ページ）



第 25 章

Analytics のダッシュボードとレポート

このセクションでは、次の点について説明します。

- Cisco Prime Collaboration Analytics ダッシュボードとレポート （537 ページ）
- Prime Collaboration Analytics ダッシュボードのトラブルシューティング （582 ページ）

CiscoPrimeCollaborationAnalyticsダッシュボードとレポート

Cisco Prime Collaboration Analytics ダッシュボードには、期間の依存関係があります。そのレポートに固有の期間（毎日、毎週、毎月）のためのデータを処理するために十分な時間が経つまで、レポートは生成できません。

Cisco Prime Collaboration リリース 11.0 以前の場合

過去 1 年以内の期間のみ、カスタム レポートを生成できます。1 年以上時間が経ったすべてのレポート データは削除されます。

Cisco Prime Collaboration Analytics を初めて起動するときに、Cisco Prime Collaboration Analytics ダッシュボードにデータを表示させるには、次の手順を実行する必要があります。

- デバイス検出
- **Cisco Prime Collaboration リリース 11.1 以前の場合**

  セッションのインポート
- 会議のインポート
- デバイスのポーリング

これらのタスクの詳細については、『Cisco Prime Collaboration Assurance ガイド - Advanced』を参照してください。

Cisco Prime Collaboration Analytics のユーザ役割

ユーザ ロールは、ユーザがアクセスできるタスクの許可を定義するために使用されます。

ユーザには、次のいずれかのロールを割り当てることができます。

- ヘルプデスク：[分析（Analytics）] メニューにはアクセスできません。
- オペレータ：すべてのダッシュボードを表示できますが、スケジュール済みレポートを編集および削除するためのアクセス権はありません。また、オペレータのユーザには設定機能がありません。
- レポート ビューア：キャパシティ分析、ライセンス使用状況、マイ ダッシュボード以外のすべてのダッシュボードにアクセスできます。レポート ビューアではレポートをスケジュールすることはできず、[スケジュール設定済みレポート（Scheduled Reports）] メニューにアクセスすることもできません。
- ネットワーク管理者、システム管理者、スーパー管理者—すべてのダッシュボードにアクセスし、すべての設定タスクを実行できます。

Cisco Prime Collaboration Assuranceを MSP モードで導入した場合、[カスタム レポート ジェネレータ（Custom Report Generator）] メニューにはアクセスできません。

Cisco Prime Collaboration Assurance のロールとその機能の詳細については、『Cisco Prime Collaboration Assurance Advanced ガイド』の「Cisco Prime Collaboration Assurance-高度なユーザ ロール」を参照してください。

ユーザ ロールとタスクには、Cisco Prime Collaboration Analyticsのユーザ ロールとマップされているタスクが一覧表示されています。

グローバル顧客の選択

Cisco Prime Collaboration リリース 11.5 以降の場合

このセクションは、Cisco Prime Collaboration Assurance を MSP モードで導入した場合のみ適用されます。

Cisco Prime Collaboration Assurance のホームページでは、顧客を選択できます。顧客を選択するには、右上の [設定（Settings）] アイコンをクリックし、**[顧客（Customer）]** を選択します。**[顧客（Customer）]** ダイアログボックスで対象の顧客名を選択し、**[OK]** をクリックします。選択した顧客に基づき、データが分析ダッシュボードに表示されます。

グローバル顧客選択の詳細については、『Cisco Prime Collaboration Assurance Advanced ガイド』の「グローバル顧客選択」セクションを参照してください。

グローバル ドメインの選択

Cisco Prime Collaboration リリース 11.5 以降の場合

このセクションは、Cisco Prime Collaboration Assurance を Enterprise モードで導入した場合のみ適用されます。

Cisco Prime Collaboration Assurance のホームページでは、ドメインを選択できます。選択したドメインに基づき、データが分析ダッシュボードに表示されます。

グローバルドメイン選択の詳細については、『Cisco Prime Collaboration Assurance Advanced ガイド』の「Assurance のグローバルドメイン選択」セクションを参照してください。

ユーザ インターフェイス

Prime Collaboration Analytics ユーザ インターフェイス (UI) を使用できます

- グラフ モードまたはグリッド モードでダッシュレットを表示する
- データをエクスポートする
- チャート タイプを変更する
- 詳細ビューまたはクイック ビューを表示する（これによりチャートやグリッドの表示を選択することができる）
- 対応する円グラフや棒グラフの 1 区画に関するデータのヒントを表示する
- ダッシュレットの最大化

[Filters（フィルタ）*]* ペインでクラスタおよび期間に基づいて表示されるデータをフィルタリングできます。

ダッシュレットの右上隅にある最大化アイコンをクリックすることで、ダッシュを最大化することができます。最大化アイコンをクリックすると、ダッシュレットが新しいタブで表示されます。

デフォルトでは、すべての分析ダッシュレットのレイアウト テンプレートは、50/50 として設定されます。最適なビューを表示するには、この設定を変更することを推奨しません。ただし、カスタム レイアウトを設定する場合は、右上の アイコンをクリックし、**[Layout Template]** を選択して、目的のレイアウトを選択します。

クイック ビュー

円グラフや棒グラフの 1 区画をクリックして、対応するエンドポイントのクイック ビューを起動できます。クイック ビューには、選択したエンドポイントに対してのみグラフが表示されます。ダッシュレット ビューと同様に、クイック ビューでも以下の処理が可能です。

- グラフ モードまたはグリッド モードでダッシュレットを表示する
- チャート タイプを変更する
- データをエクスポートする
- 詳細ビューを起動する

グローバル フィルタ オプション

フィルタ オプションは、各ダッシュレットの UI の左上から使用できます。期間（過去 1 週間、1 か月など）に基づいてすべてのダッシュレットに対して表示されるデータ、およびダッシュレットのタイプに基づいてその他の属性に対して表示されるデータをフィルタリングすることができます（例：トラフィック分析ダッシュボードでのコール タイプ（音声またはビデオ））。

（注）

Cisco Prime Collaboration リリース 11.1 以前の場合

グローバル フィルタはテクノロジ導入のダッシュボードにあるメトリックに適用されません。

詳細分析

Prime Collaboration Analytics には、各ダッシュレット（エンドポイント、デバイス、テクノロジ使用率など）の詳細な分析が用意されています（右下の [See Details] をクリックしてください）。

[Detailed Analysis] ページには、[Metrics and Filter] ペインと [Graph] ペインがあります。

[Metrics and Filter] ペイン：期間、コールの方向、コール タイプ、コールのステータス、計算（絶対値またはパーセンテージ）、コール件数、コール期間、エンドポイント タイプ、エンドポイント モデル、導入のステータス、クラスタ、拠点/デバイス プールに基づいてデータをフィルタリングできます。

（注）

キャパシティ分析のすべてのダッシュレットで、カスタム グループ、使用率、個別のグラフ（各エンティティを縦に 1 つずつ表示し、1 ページあたりのグラフ数は 20 個に制限される）、またはマージされたグラフ（すべてのエンティティを 1 つのグラフに表示する）を使用して、結果をフィルタリングすることができます。[Keep selected time span in sync across all graphs] を選択すると、すべてのグラフでカスタム日付を同期させることができます。

[Export] オプション。[Metrics and Filter] ペインの後で右上に表示され、エクスポートをスケジュールすることができます。スケジュールの設定に従ってダッシュレットのレポートを生成したり、それらのレポートをダウンロードしたり、指定の電子メール ID に送信したりできます（レポートの生成が失敗した場合は、失敗の通知を送信することもできます）。スケジュールされたレポートを、設定されている sFTP サーバへ送信することもできます。sFTP サーバを設定するには、「sFTP サーバの設定」を参照してください。チャートのデータは CSV 形式または PDF でエクスポートできます。表ベースのダッシュレットのデータは、CSV 形式でエクスポートできます。

[Graph] ペイン：表示されるグラフは、[Filter] ペインの各パラメータについての値セットに基づいてます。グラフの下のスライダには、（[Filter] ペインで設定される）目的の期間が表示されます。ユーザはスライダをドラッグして特定の期間を拡大する（期間の幅を狭くする）ことも、X 軸および Y 軸の値を変更することもできます。これにより、データがその期間に対してフィルタリングされます。

表形式のビュー：Prime Collaboration Analytics にはデータを表形式で表示するオプションがあります。これによりデータのより深い、詳細な分析（詳細なコール レコード、時間ごとのネットワーク使用率、エンドポイントの情報など）を提供することができます。詳細分析で、スライダの下に表示されている凡例またはシリーズをクリックしたとき、またはグラフ上の任意の場所をダブルクリックしたときに、表形式のビューがポップアップ表示されます。また、テーブルのデータをフィルタリングすることも、エクスポートすることもできます。

（注）

- 詳細ビューでは、サブゾーンが設定されていない場合には必ず、Cisco VCS 登録エンドポイントのダッシュレットにデバイス プールと拠点が表示されます。Cisco VCS クラスタまたはサブゾーンの詳細が次のダッシュレットに表示されます。
  - [トラフィック分析のすべてのダッシュレット（All dashlets in Traffic Analysis）]
  - サービス エクスペリエンスのすべてのダッシュレット。
  - —Technology Adoption で Endpoint Model Endpoints Deployment Summary 別となっている Deployment Distribution のすべてのダッシュレットを除きます。
  - 使用頻度が最も低いエンドポイント タイプ（資産の使用率）。

  Cisco VCS でサブ ゾーンが設定されていない場合、拠点、コーデック、およびデバイス プールの詳細が VCS_Unknown として表示されます。障害の詳細は、Cisco VCS に登録されたコールには適用されないため、詳細ビューにはゼロとして表示されます。

- **Cisco Prime Collaboration リリース 11.1 以前の場合**

  Call Detail Records（CDR）ベースのダッシュレットの詳細ビューには、過去 30 日間のみの CDR または Call Management Records（CMR）のデータが表示されます。ダッシュレットには、30 日より前のエンドポイントのコールに関する詳細は表示されませんが、、13 か月、または 56 週間の間に集計された CDR または CMR データが利用できます。

  —Call Detail Records（CDR）ベースのダッシュレットの詳細ビューには、過去 30 日間のみの CDR または Call Management Records（CMR）のデータが表示されます。ダッシュレットには、30 日より前のエンドポイントのコールに関する詳細は表示されませんが、3 か月または 12 週間の間に集計された CDR または CMR データが利用できます。

- IP アドレスとディレクトリ番号のフィルタ機能があるダッシュレットでは、次の順序で詳細を入力します。
  - IP アドレスの形式は x.x.x.x である必要があり、範囲はこれら 2 つの値を除く 0.0.0.0 と 255.255.255.255 の間に設定できます。また、特殊文字を含めることはできません。
  - ディレクトリ番号に、+、@、.（ピリオド）を使用できます。

- キャパシティ分析や資産の使用率などの一部のダッシュボード（使用頻度が最も低いエンドポイントは除く）では、最大 100 個のデータを表示することができます。フィルタ結果が 100 件を超える場合は、エラー メッセージが表示されます。また、エンドポイント タイプと拠点に対してフィルタ オプションがサポートされている場合は、最大値の 100 は拠点に対して適用され、エンドポイントには適用されません。
- データをエクスポートする場合は、すべての分析データがエクスポートされます。フィルタ パラメータは、エクスポートされたデータに対してではなく、UI に表示されているデータに対してのみ適用されます。

ヒントを使用して、グラフィカル ビューを便利にカスタマイズすることができます。

レポートのスケジュール、エクスポート、およびインポート

各ダッシュレットの左下に表示されるドロップダウンアイコンには、レポートの印刷、エクスポート、およびスケジュールを選択するオプションがあります。スケジュールの設定に従ってダッシュレットのレポートを生成したり、それらのレポートをダウンロードしたり、指定の電子メール ID に送信したりできます（レポートの生成が失敗した場合は、失敗の通知を送信することもできます）。 スケジュールされたレポートを、設定されている sFTP サーバへ送信することもできます。sFTP サーバを設定するには、「sFTP サーバの設定」を参照してください。

レポート生成のジョブをスケジュールする場合は、開始時間ではなく、開始日のみを選択できます。Prime Collaboration は、Job Scheduler によりジョブをスケジュールします。定期ジョブは、（繰り返しの間隔には関係なく）その日に新しく作成されたレポートに対して 60 分ごとにチェックを行い、レポートを実行します。デフォルトでは、繰り返しの間隔によってその日に 1 回だけ新しく作成されたレポートは、それぞれのタイムゾーンの午後 10 時 59 分にもう一度実行されます。

繰り返しがスケジュールされているすべてのレポート（毎日、毎週、毎月）は、繰り返しの間隔に基づいて各タイムゾーンの午前 5 時～8 時に毎日実行されます。これらのレポートは、レポートの実行にかかった時間に基づいて、低および高の優先順位が付けられます。実行時間が長いレポートは優先順位が「低」と分類され、実行時間が短いレポートは優先順位が「高」として分類されます。優先順位が高いレポートは一連のレポートの中で最初に実行され、その後は優先順位が高い順に実行されます。優先順位が低いレポートは、4 件単位で実行されます。

チャートのデータは CSV 形式または PDF でエクスポートできます。表ベースのダッシュレットのデータは、CSV 形式でエクスポートできます。レポートごとに保存できるインスタンスの数を指定することもできます。インスタンス数が指定した制限に達すると、時系列順で最初に保存されたレポートが消去されます。

1. **Bottom Table でデータのパージング**：パージングでは、Bottom Table（BT）のデータは 35 日後に削除されますが、実行履歴には、スケジュール済みレポートが生成したものと同じ回数が表示されます。
2. **スケジュール済みレポートのカスタム間隔**：スケジュール済みレポートを生成すると、スケジュールしたときと同じ間隔を示すレポートが生成されます。

（注） したがって、カスタム間隔ではレポートをスケジュール設定しないよう推奨します。

顧客ロゴの管理

Cisco Prime Collaboration リリース 11.5 以降の場合

Cisco Prime Collaboration Analytics を MSP モードで展開している場合は、顧客にロゴを割り当てることができます。これらのロゴは、ダッシュレットを使用して（スケジュールまたはエクスポートによって）生成されたレポートに表示されます。生成されたレポートには、グローバル カスタマー選択で選択された顧客のロゴが表示されます。

（注） 顧客のロゴは、PDF 形式のレポートでのみ使用できます。

顧客のロゴは、アップロード、削除、およびリセットが可能です。

顧客のロゴをアップロードするには、次のようにします。

始める前に

このタスクを実行するには、管理者特権が必要です。

ステップ 1 [分析管理（Analytics Administration）] > [顧客のロゴのアップロード（Upload Customer Logo）] を選択します。

ステップ 2 適切な顧客名を選択します。

ステップ 3 [参照（Browse）] をクリックして、適切な画像を選択します。

（注） .jpg、.jpeg、.bmp、または .gif の形式の画像のみをアップロードできます。

ステップ 4 [送信（Submit）] をクリックして、画像を顧客のロゴとして保存します。

ロゴを削除するには、[ロゴの削除（Delete Logo）] をクリックします。[リセット（Reset）] をクリックすると、ロゴを更新できます。

sFTP サーバの設定

sFTP サーバを設定するには、次の手順を実行します。

始める前に

Cisco Prime Collaboration Analytics を MSP モードで展開した場合は、次のことを確認してください。

- ユーザ <*userid*> は、sFTP サーバで使用できます。
- /<*path*>/<*userid*> フォルダは sFTP サーバで利用可能であり、その特定のユーザ <*userid*> および管理者だけがアクセスできます。

ステップ 1 [Analytics Administration] > [sFTP Settings] を選択します。

ステップ 2 [sFTP 設定（sFTP Settings）] ページで、必要な詳細を入力します。フィールドの説明については、表 66 : sFTP 設定フィールド （545 ページ）を参照してください。

ステップ 3 sFTP サーバへの接続を確認するには、[Test Connection] をクリックします。

（注） MSP モードでは、テスト接続を使用して、/< *path* >/< *userid* > フォルダが sFTP サーバで使用可能かどうかを検証できます。

ステップ 4 正常に接続したら、[Save] をクリックします。

Cisco Prime Collaboration リリース 11.1 以前の場合

MSP モードでは、オペレータのユーザは [分析管理（Analytics Administration）] メニューにアクセスできず、sFTP サーバを設定することもできません。

表 *66 : sFTP* 設定フィールド

フィールド	説明
sFTP サーバ（IP アドレス）	スケジュール済みのレポートを保存する必要がある sFTP サーバの IP アドレス。
sFTP Port	sFTP サーバのポート番号。
パス（ディレクトリ）	スケジュール済みレポートを保存する必要がある sFTP サーバ内のディレクトリ パス。 Cisco Prime Collaboration Analytics を MSP モードで展開した場合は、レポートが /<*path*>/<*userid*> の場所に保存され、Cisco Prime Collaboration Analytics を Enterprise モードで展開した場合は、レポートが /<*path*> の場所に保存されます。
User Name	sFTP サーバにアクセスするためのユーザ名。
Password	sFTP サーバにアクセスするためのパスワード。

Cisco Prime Collaboration Analytics ダッシュレットのデータ入力の前提条件

Cisco Prime Collaboration Analytics ダッシュレットに入力するデータに対して、次の前提条件が満たされていることを確認します。

- Unified CM および Cisco VCS に登録されているエンドポイントが検出される（および**インベントリ**）。
- Unified CM および Cisco VCS に登録されているエンドポイント用の CDR レコードが利用可能であること (**[レポート（Reports）] > [CDR および CMR レポート（CDR & CMR Reports）]**。

- 登録した Unified CM のデータが、で収集できる。**[アラームおよびレポート管理（Alarm & Report Administration）] > [CDS ソース設定（CDR Source Settings）] > [通話品質データ ソース管理（Call Quality Data Source Management）]**。
- それぞれのダッシュボードでグローバルフィルタを空に設定して、データの入力を検証する。
- Analytics は、選択された期間について収集された履歴データを使用する。日、週、および月に対するフィルタを選択した場合、データは現在の日、週、および月を除いて表示される。

テクノロジー導入

これまでに行われたテクノロジー投資を検証するために、テクノロジー導入ダッシュボードを使用します。このダッシュボードはまた、将来の投資決定に使用できる重要な意思決定を支援するメトリックを提供します。

前提条件：Unified CM および Cisco VCS に登録されているエンドポイントが検出されていること。

データ ソース：このダッシュレットのデバイスの詳細は、Prime Collaboration のインベントリから収集され、コールの詳細は Unified CM および Cisco VCS CDR から収集されます。

このダッシュボードのすべてのダッシュレットは Unified CM と VCS に登録されたエンドポイントのデータを表示します。

不明なエンドポイントの導入の詳細については、テクノロジー導入ダッシュボードに表示されません。

テクノロジー導入ダッシュボードは、組織で導入された音声エンドポイントやビデオエンドポイントの概要情報およびスナップショット ビューを提供するメトリックを表示します。

テクノロジー導入ダッシュボードには、次のメトリックが表示されます。

メトリック	次の概要情報を提供します。
導入されたビデオ エンドポイント	• 使用中のビデオ エンドポイント合計 • 過去 1 か月のエンドポイント数の変更 • 導入されたビデオ エンドポイントの割合
ビデオ コール分数	• ビデオ コールの合計時間 • 過去 12 週間のビデオ コール時間の変更 • ビデオ コールの使用状況の傾向

導入された音声エンドポイント	• 音声エンドポイントの合計数 • 過去 1 か月のエンドポイント数の変更 • 導入された音声エンドポイントの割合
音声コール分数	• 音声コールの合計時間 • 過去 12 週間の音声コール時間の変更

メトリックを表示する期間を選択するには、ドロップダウン リストを使用します。

次のダッシュレットは、テクノロジー導入ダッシュボードで使用可能です。

エンドポイント モデルによる導入の分配

Cisco Prime Collaboration リリース 11.1 以前の場合

このダッシュレットは設定された実行中のエンドポイントの導入のトレンドを示します。

- 登録ステータスに関係なく、Cisco Prime Collaboration Assurance で管理されるすべてのエンドポイントは、設定エンドポイントとして分類されます。
- Cisco Prime Collaboration Assurance 内の登録済みか、部分的に登録された状態にあるエンドポイントは、アクティブなエンドポイントです。

デフォルトでは、このダッシュレットに Cisco Prime Collaboration Assurance がインストールされた日付から現在の日付までのすべてのエンドポイントのグラフが表示されます。週ごとにデータをフィルタ処理できます。期間を 7 日前に選択すると、Prime Collaboration をインストールした日付から現在の日付までに展開されたすべてのエンドポイントがグラフに表示されます（7 日前）。

一例として、CTS 1000 シリーズなどの特定のエンドポイント モデルについて一定期間の追加/展開における増加レートを判断することができます。

（注） **期間**のグローバル フィルタはこのダッシュレットに適用されません。

デバイスの詳細（モデル番号、バージョンなど）は、Prime Collaboration インベントリから収集され、また SNMP および HTTP を使用してエンドポイントをポーリングしてしても収集されます。このデバイス情報は分析データベースで格納され、モデルに基づいてエンドポイントをグループ化するために使用されます。こうして収集した詳細情報は円グラフとして表示されます。

エンドポイント タイプ、エンドポイント モデル、デバイス プール、クラスタまたは拠点に基づいて詳細ビューで導入データをフィルタリングできます。特定のエンドポイント モデルの実行中および設定されているデバイスの累積数も表示できます。

Cisco VCS に登録されている Cisco Jabber 電話では、登録ステータスに関係なく、実行数と設定したエンドポイント数は同じになります。これは、Cisco Jabber のステータスが登録されて

いない場合、インベントリが [Deleted] 状態に移行するためです。その他の電話では、（ソフトクライアント CSF や CUPC などと同様に）、24 時間以上ステータスが登録されていない場合のみデバイスのステータスが「Deleted」になります。

エンドポイント展開の概要

Cisco Prime Collaboration リリース 11.5 以降の場合

このダッシュレットは設定された実行中のエンドポイントの導入のトレンドを示します。

- 登録ステータスに関係なく、Cisco Prime Collaboration Assurance で管理されるすべてのエンドポイントは、設定エンドポイントとして分類されます。
- Cisco Prime Collaboration Assurance 内の登録済みか、部分的に登録された状態にあるエンドポイントは、アクティブなエンドポイントです。

デフォルトでは、このダッシュレットに Cisco Prime Collaboration Assurance がインストールされた日付から現在の日付までのすべてのエンドポイントのグラフが表示されます。週ごとにデータをフィルタ処理できます。期間を 7 日前に選択すると、Cisco Prime Collaboration Assurance をインストールした日付から現在の日付までに展開されたすべてのエンドポイントがグラフに表示されます（7 日前）。

一例として、CTS 1000 シリーズなどの特定のエンドポイント モデルについて一定期間の追加/展開における増加レートを判断することができます。

（注） **期間**のグローバル フィルタはこのダッシュレットに適用されません。

デバイスの詳細（モデル番号、バージョンなど）は、Cisco Prime Collaboration Assurance インベントリから収集され、SNMP または HTTP を使用したエンドポイントのポーリングによっても収集されます。このデバイス情報は分析データベースで格納され、モデルに基づいてエンドポイントをグループ化するために使用されます。こうして収集した詳細情報は円グラフとして表示されます。

エンドポイント タイプ、エンドポイント モデル、デバイス プール、クラスタまたは拠点に基づいて詳細ビューで導入データをフィルタリングできます。特定のエンドポイント モデルの実行中および設定されているデバイスの累積数も表示できます。

Cisco VCS に登録されている Cisco Jabber 電話では、登録ステータスに関係なく、実行数と設定したエンドポイント数は同じになります。これは、Cisco Jabber のステータスが登録されていない場合、インベントリが [Deleted] 状態に移行するためです。その他の電話では、（ソフトクライアント CSF や CUPC などと同様に）、24 時間以上ステータスが登録されていない場合のみデバイスのステータスが「Deleted」になります。

エンドポイント モデルによるコール分配

Cisco Prime Collaboration リリース 11.1 以前の場合

このダッシュレットはエンドポイント モデルごとのコールの量に基づいてコール分配を表示します。次のようなコールの詳細を表示できます。

- 完了および失敗したコールを含む、試行されたすべてのコール。
- エンドポイントから発信され成功したすべてのコール。
- ドロップして接続に失敗したコール。
- 接続に失敗したすべてのコール。

このダッシュレットのデバイスの詳細は、Prime Collaboration のインベントリから収集され、コールの詳細は Unified CM および Cisco VCS CDR から収集されます。

デバイス プール、IP アドレス、エンドポイント タイプ、エンドポイント モデル、コール タイプ、コール ステータス、コール方向、コール数、コール期間、クラスタ、ユーザ ID または拠点に基づいて詳細ビュー ページのコール分配の詳細をフィルタリングできます。

クラスタ フィルタは、Cisco VCS をサポートしていません。

上記の「コール方向」は、着信または発信を意味します。これは、コールを発信するエンドポイントまたは拠点の視点に基づいて決定されます。たとえば、エンドポイント A がエンドポイント B をコールした場合、エンドポイント A の視点では発信コール、エンドポイント B の視点では着信コールです。

エンドポイント モデルごとのコール量

Cisco Prime Collaboration リリース 11.5 以降の場合

このダッシュレットはエンドポイント モデルごとのコールの量に基づいてコール分配を表示します。次のようなコールの詳細を表示できます。

- 完了および失敗したコールを含む、試行されたすべてのコール。
- エンドポイントから発信され成功したすべてのコール。
- ドロップして接続に失敗したコール。
- 接続に失敗したすべてのコール。

このダッシュレットのデバイスの詳細は、Prime Collaboration のインベントリから収集され、コールの詳細は Unified CM および Cisco VCS CDR から収集されます。

デバイス プール、IP アドレス、エンドポイント タイプ、エンドポイント モデル、コール タイプ、コール ステータス、コール方向、コール数、コール期間、クラスタ、ユーザ ID または拠点に基づいて詳細ビュー ページのコール分配の詳細をフィルタリングできます。

クラスタ フィルタは、Cisco VCS をサポートしていません。

上記の「コール方向」は、着信または発信を意味します。これは、コールを発信するエンドポイントまたは拠点の視点に基づいて決定されます。たとえば、エンドポイント A がエンドポイント B をコールした場合、エンドポイント A の視点では発信コール、エンドポイント B の視点では着信コールです。

エンドポイント タイプによるコール分配

Cisco Prime Collaboration リリース 11.1 以前の場合

このダッシュレットはエンドポイント タイプの音声エンドポイントやビデオ エンドポイントに基づいてコール分配を表示します。

音声エンドポイントは、音声通話の発信および受信ができるデバイスです。音声 IP 電話、ワイヤレス IP 電話と個人の通信エンドポイントは、音声エンドポイントとして分類されます。

ビデオ エンドポイントは、ビデオ コールの発信および受信ができるデバイスです。多目的テレプレゼンス、イマーシブ テレプレゼンス、パーソナル テレプレゼンス、モバイル ビデオ、デスクトップ ビデオ デバイスは、ビデオ エンドポイントとして分類されます。

Cisco Prime Collaboration Assurance でサポートされるオーディオおよびビデオ エンドポイントの一覧については、『Cisco Prime Collaboration Assurance でサポートされているデバイス』を参照してください。

このダッシュレットのデバイス詳細は Prime Collaboration のインベントリから収集され、このダッシュレットに関するコール詳細は Unified CM および Cisco VCS CDR から取得されます。

デバイス プール、URI、ディレクトリ番号、IP アドレス、エンドポイント タイプ、エンドポイント モデル、コール タイプ、コール ステータス、コール方向、コール数、通話時間、クラスタ、ユーザ ID、または拠点に基づいて詳細ビュー ページのコール分配の詳細をフィルタリングできます。

エンドポイント タイプごとのコール量

Cisco Prime Collaboration リリース 11.5 以降の場合

このダッシュレットはこのダッシュレットはエンドポイント タイプの音声エンドポイントやビデオ エンドポイントに基づいてコール分配を表示します。

音声エンドポイントは、音声通話の発信および受信ができるデバイスです。音声 IP 電話、ワイヤレス IP 電話と個人の通信エンドポイントは、音声エンドポイントとして分類されます。

ビデオ エンドポイントは、ビデオ コールの発信および受信ができるデバイスです。多目的テレプレゼンス、イマーシブ テレプレゼンス、パーソナル テレプレゼンス、モバイル ビデオ、デスクトップ ビデオ デバイスは、ビデオ エンドポイントとして分類されます。

Cisco Prime Collaboration Assurance でサポートされるオーディオおよびビデオ エンドポイントの一覧については、『Cisco Prime Collaboration Assurance でサポートされているデバイス』を参照してください。

このダッシュレットのデバイス詳細は Prime Collaboration のインベントリから収集され、このダッシュレットに関するコール詳細は Unified CM および Cisco VCS CDR から取得されます。

デバイス プール、URI、ディレクトリ番号、IP アドレス、エンドポイント タイプ、エンドポイント モデル、コール タイプ、コール ステータス、コール方向、コール数、通話時間、クラスタ、ユーザ ID、または拠点に基づいて詳細ビュー ページのコール分配の詳細をフィルタリングできます。

テクノロジーの使用

このダッシュレットは、音声とビデオ両方の使用の傾向を表示します。コール数が最大値のエンドポイントも表示します。各週のデータをグラフまたは表形式で表示できます。デフォルトでは、過去 1 か月のデータが表示されます。

このダッシュレットのエンドポイントの詳細は、Prime Collaboration のインベントリから収集され、コールの詳細は Unified CM および Cisco VCS CDR から収集されます。

詳細ビューで、音声とビデオの使用率を計算するために使用する式は次のとおりです。

エンドポイント数 >= 1 週間のコール ステータスが同じコール数（失敗、ドロップ、完了、試行）/デバイスの数 >= 1 週間のコール数（同じモデルとコール タイプ） * 100。

コール タイプ、URI、ディレクトリ番号、エンドポイント モデル、コール ステータス、使用状態、拠点、デバイス プール、クラスタ、ユーザ ID、または IP アドレスに基づいて詳細ビュー ページの詳細をフィルタリングできます。

資産使用状況

このダッシュボードでは、資産の使用率を追跡できます。たとえば、エンドポイントが効果的に割り当てられ、使用されているかどうかなどを見極めるのに役立ちます。

前提条件：Unified CM および Cisco VCS に登録されているエンドポイントが検出されていること。

データ ソース：このダッシュレットのデバイスの詳細は、Prime Collaboration のインベントリから収集され、コールの詳細は Unified CM および Cisco VCS CDR から収集されます。

資産使用状況ダッシュボードでは、次のダッシュレットを使用できます。

使用頻度が最も低いエンドポイント タイプ

このダッシュレットは 1 週間当たりに発信されたコール数に基づいて使用頻度が最も少ないエンドポイント タイプを表示します。デフォルトでは、ダッシュレットには使用されていないエンドポイント（コールがないエンドポイント）のみが表示されます。ダッシュレット ビューに表示される「週当たりのコール数が x 未満」のカテゴリには、使用されていないエンドポイントおよび週当たりのコール数が x 件のエンドポイントが含まれます。

このダッシュレットには、Unified CM および VCS に登録されているエンドポイントのデータが表示されます。このダッシュレットのデバイス詳細は Prime Collaboration のインベントリから収集され、コールの詳細は CDR から収集されます。

詳細ビューには、週次に集約されたデータのみが表示されます。エンドポイント タイプ、エンドポイント モデル、使用ステータス、デバイス プール、拠点、ユーザ ID、またはクラスタに基づいて詳細ビュー ページのデータをフィルタリングできます。

（注） 詳細ビュー グラフの週当たりの未使用のエンドポイントに関して表示されるデータは、詳細ビューの使用頻度が最も低いエンドポイント タイプ テーブルと同期していません。これは、使用頻度が最も低い Least Used Endpoint Types レポートのテーブルには、選択された時間フィルタの集計データが表示されるためです。これは、資産使用のダッシュレット ビューと同じです。

ビデオ テレプレゼンス ルームの使用率

使用率が最も高いエンドポイントと最も低いエンドポイントを追跡することができます。このダッシュレットには、エンドポイント名、セッション数、使用期間、および1週間の使用率のリストが表示されます。期間、エンドポイントタイプ、および使用率のパーセンテージでデータをフィルタリングできます。

次を使用して、管理対象の各エンドポイントについて、1 日あたりの作業時間（デフォルトは 8 時間）および 1 週間あたりの作業日数（デフォルトは 5 日）をカスタマイズできます。**[使用率の変更（Change Utilization）] ([アシュアランス レポート（Assurance Report）] > [Telepresence レポート（Telepresence Report）] > [エンドポイント使用率レポート（Endpoint Utilization Report）])**。これらの値は、テレプレゼンス ルームについてのアセットの使用率を分析する場合に使用されます。

マウスをエンドポイント名または使用率の上におくと、クイック ビューを起動することができます。ここではグラフとグリッド ビューが表示され、セッション数、期間、および使用率のパーセンテージが示されます。

詳細な分析では、表示された結果を期間、すべてのエンドポイント、または指定したエンドポイントタイプ、パーセンテージまたは絶対値、個別またはマージされたグラフでフィルタリングできます。すべてのエンドポイントを選択した場合は、使用率のパーセンテージによってフィルタリングすることもできます。

No Show Video TelePresence エンドポイント

スケジュールされたセッションに参加しなかったエンドポイントを特定することができます。このダッシュレットには、スケジュールされた完全なセッションに基づいたデータが表示されます。このダッシュレットで、スケジュールされたすべてのセッション、スケジュールされたセッションで開催されたもの、および不参加のセッション（スケジュールされたが開始されなかったセッション、およびスケジュールされ、開催されたセッションだがセッションに含まれているエンドポイントが参加しなかったもの）を表示することができます（この列のデータをパーセンテージおよび絶対値で表示できます）。不参加のエンドポイントの件数が1以上のものが一覧で表示されます。期間、エンドポイント タイプ、および不参加によって、データをフィルタリングできます。

詳細な分析では、データを期間、エンドポイント名、エンドポイントタイプ、エンドポイントモデル、不参加（絶対値とパーセンテージ）、クラスタ、拠点、デバイスプールでフィルタして、エンドポイントの不参加、および不参加のパーセンテージの傾向を確認できます。エンドポイントの凡例をクリックすると、スケジュールセッションの合計数と、エンドポイントのモデルとタイプ、およびエンドポイントの参加と不参加の件数を確認できます。

（注） このダッシュレットは、Cisco Prime Collaboration Analytics の MSP モードではサポートされていません。

Cisco Prime Collaboration リリース 12.1 SP2 以降の場合

No Show Video Telepresence エンドポイントの前提条件。

（注） Conference Diagnostics を有効にしてデータが入力できることを確認します。

次は、No Show Video Telepresence エンドポイントの要件です。

- Unified CM および Cisco VCS は、Managed 状態にある必要があります。
- MCU などのエンドポイントとコントローラは、Managed 状態にある必要があります。
- デバイスの可視性を 「Full Visibility」 状態に設定します。
- JTAPI が Unified Communications Manager で設定されている必要があります。Unified Communications Manager で JTAPI を有効にする方法については、「Cisco Prime Collaboration Assurance のデバイス設定」を参照してください。
- Cisco Prime Collaboration Assurance サーバが、Cisco VCS でフィードバック サーバとして登録されている必要があります。
- 会議の診断と音声電話機能の模擬テストを正しく実行するには、Cisco Prime Collaboration Assurance Service Pack 1 バンドルを適用する前に、CUCM がリストされているバージョンであることを確認してください。詳細については、12.1 Service Pack 1 の『Cisco Prime Collaboration Assurance でサポートされているデバイス』を参照してください。

No Show Video TelePresence エンドポイント

Cisco Prime Collaboration リリース 11.1 以降の場合

スケジュールされたセッションに参加しなかったエンドポイントを特定することができます。このダッシュレットには、スケジュールされた完全なセッションに基づいたデータが表示されます。このダッシュレットで、スケジュールされたすべてのセッション、スケジュールされたセッションで開催されたもの、および不参加のセッション（スケジュールされたが開始されなかったセッション、およびスケジュールされ、開催されたセッションだがセッションに含まれているエンドポイントが参加しなかったもの）を表示することができます（この列のデータをパーセンテージおよび絶対値で表示できます）。不参加のエンドポイントの件数が 1 以上のものが一覧で表示されます。期間、エンドポイント タイプ、および不参加によって、データをフィルタリングできます。

詳細な分析では、データを期間、エンドポイント名、エンドポイントタイプ、エンドポイントモデル、不参加（絶対値とパーセンテージ）、クラスタ、拠点、デバイスプールでフィルタして、エンドポイントの不参加、および不参加のパーセンテージの傾向を確認できます。エンドポイントの凡例をクリックすると、スケジュールセッションの合計数と、エンドポイントのモデルとタイプ、およびエンドポイントの参加と不参加の件数を確認できます。

（注） このダッシュレットは、Cisco Prime Collaboration Analytics の MSP モードではサポートされていません。

トラフィック分析

トラフィック分析のダッシュボードは、組織内のさまざまなユーザ、部門、テクノロジーの使用状況を表示します。これは、さまざまな組織単位または部門にわたってビジネス コストを計画し、割り当てるのに役立ちます。

データ ソース：トラフィック分析のダッシュボードのダッシュレットのコール詳細は、Cisco Unified Communications Manager が生成する CDR から取得されます。

（注） 詳細ビューでは、フィルタは上位 N に基づいています。下部のテーブルには、[詳細ビュー（Detail View）] ページで選択した他のフィルタ条件に基づき、すべてのレコードが表示されます。ただし、raw データはデータベースに 35 日間のみ保管されます。下部のテーブルには、対応するデータが表示されます。

次のダッシュレットは、トラフィック分析ダッシュボードで使用可能です。

上位 N の発信者

このダッシュレットは、Prime Collaborationの管理による導入内で、ディレクトリ番号から他の任意の番号にコールされた合計数に基づき、コール発信元の上位 N つの番号を一覧表示します。

ディレクトリ番号、コール タイプ、コール数、通話時間、クラスタ、拠点、デバイス プールまたはエンドポイントの詳細（IP、発信者番号、または送信元URIなど）に基づいて詳細ビューページに表示されるデータをフィルタリングできます。Prime Collaboration で管理されたエンドポイントのディレクトリ番号は表示されますが、外部のディレクトリ番号は表示されません。

絶対値または割合モードのいずれかで、コール数または通話時間を表示できます。エンドポイントまたはユーザでそれぞれフィルタリングすると、ユーザまたは電話番号を表示することもできます。

上位 N の発信者の割合を計算するために使用する式は次のとおりです。

1 週間における特定番号のコール総数または通話時間/その週におけるすべての発信者のコール総数または通話時間* 100。

このダッシュレットには、Unified CM および VCS に登録されているエンドポイントのデータが表示されます。

詳細ビューで表示されるズーム セレクタ グラフを使用して、グラフの時間ウィンドウ（X 軸）ポインタを調整し、その特定の電話番号からの選択した期間のコールの詳細を表示できます。

また、グローバル クラスタ フィルタを使用して、個別のクラスタの上位 N の発信者を表示することができます。

上位 N のダイヤル番号

このダッシュレットは、指定された期間の宛先に基づき、かけた番号の上位N位を示します。次のような上位 N の番号を確認できます。

- 呼び出し回数（コール数）が最も高い番号
- コール時間（通話時間）が最も長い番号

このダッシュレットには、Unified CM および VCS に登録されているエンドポイントのデータが表示されます。

ディレクトリ番号、コールタイプ、コール数、通話時間、クラスタ、または拠点に基づいて詳細ビューに表示される詳細をフィルタリングできます。Prime Collaboration で管理されたエンドポイントのディレクトリ番号は表示されますが、外部のディレクトリ番号は表示されません。

上位 N のオフネット トラフィック拠点

このダッシュレットには拠点ごとのオフネットとオンネット トラフィックの傾向が表示されます。

[詳細ビュー（Detailed View）] ページに表示されるデータを、オフネットまたはオンネット トラフィック、コール タイプ、コール カウント、通話時間、クラスタ、場所、デバイス プール, エンドポイントの詳細（IP、ディレクトリ番号、送信元 URI など）、通話方向、ユーザ ID に基づきフィルタすることができます。

（注） また、着信コールまたは発信コールの方向に基づき、詳細ビューのデータをフィルタすることもできます。着信コールはゲートウェイが CUCM から受信したコールであり、発信コールはゲートウェイから CUCM へと発信されたコールです。したがって、着信コールにフィルタをかける場合は、発信者または発信者のエンドポイントの詳細を入力する必要があり、発信コールをフィルタする場合は、呼び出し先または宛先のエンドポイントの詳細を入力する必要があります。

エンドポイントに基づいきデータをフィルタすると、Cisco Prime Collaboration Assurance で管理されているエンドポイントのディレクトリ番号は表示されますが、外部のディレクトリ番号は表示されません。

ダッシュレット ビューで、オンネット コールの割合を計算するために使用する式は次のとおりです。

拠点でのオンネット コールの総数 / その場所のオフネット コールとオンネット コールの総数 * 100

オフネット コールの割合を計算するために使用する式は次のとおりです。

拠点でのオフネット コールの総数 / その場所のオフネット コールとオンネット コールの総数 * 100

ダッシュレットには Video Communication Server (VCS) で処理されるコールは含まれません。

オフネットとオンネット コール

Cisco Unified CM （プライベート ネットワーク）内のコールは、オンネット コールと呼ばれます。たとえば、Cisco 内部の IP Phone から別の内部 IP Phone へのコールは、オンネット コールです。オンネット コールでは、リモート Cisco Unified CM クラスタやサードパーティの SIP ベンダー製の機器と統合するために、クラスタ間トランク（ICT）または Session Initiation Protocol (SIP) トランク経由でルーティングできます。

オフネット コールは通常、専用のテレフォニー システムの外で PSTN にルーティングするコールです。ほとんどのオンネット コールがゲートウェイ経由で PSTN にルーティングされます。また、少なくとも 1 つののエンドポイントがトランクまたはゲートウェイの場合および、次のうち 1 つのエンドポイントが有効な場合、コールはオフネットとして分類できます。

- [Call Classification] パラメータが Unified Communications Manager （管理）のゲートウェイ設定またはトランクの設定で [Offnet]に設定されている。
- [Call Classification] パラメータがゲートウェイの設定またはトランクの設定で [System Default] に設定されている。
- [System Default] サービス パラメータが [Offnet] に設定されている。
- エンドポイントがアナログ ゲートウェイである。

オフネット コールの基準を満たさないコールはすべてオンネット コールと見なされます。

（注） デフォルトでは、ゲートウェイとの間のすべてのルート パターンおよびすべてのコールはオフネットとして分類されます。

上位 N コール トラフィック拠点

このダッシュレットは、コール数または通話時間に基づいてコールの最大数が上位 N の拠点を特定するのに役立ちます。

拠点（最上位 N および最下位 N の両方）、デバイス プール（最上位 N および最下位 N の両方）、IP アドレス、ディレクトリ番号、URI、コール タイプ、コール ステータス、コール数、通話時間、コール方向、ユーザ ID、またはクラスタに基づいて、上位 N の拠点を特定するのに役立ちます。

（注） ダッシュレットには、試行されたコールのみに基づいてコール拠点を表示します。完了、ドロップ、失敗したコールなどその他のステータスのフィルタリングは、詳細ビューで有効にします。

ダッシュレット ビューで、コール数が最大の拠点の割合を計算するために使用する式は次のとおりです。

拠点のコール総数または通話時間/すべての拠点のコール総数または通話時間 * 100。

コール トラフィック分析

このダッシュレットには、次の事前定義されたコール カテゴリに属しているコールの分配が表示されます。

- 外部
- 内部
- 会議
- 緊急
- 長距離
- フリーダイヤル
- H 323 （着信および発信ゲートウェイ/トランク）または MGCP （着信および発信）または SIP （着信および発信トランク）
- ボイスメール
- ローカル
- 国際

コール カテゴリを追加するには、コール カテゴリの作成の項を参照してください。

（注） コールは複数のコール カテゴリに含めることができます。たとえば、内線コールは会議コールにもできます。したがって、すべてのカテゴリに属する全コールの合計数は、レポートされた総コール数を上回る場合があります。

このダッシュレットには Unified CM で処理されるコールの詳細のみが含まれます。コール カテゴリの情報は CDR から収集されます。

ダッシュレット ビューで、コールの分配の割合を計算するために使用する式は次のとおりです。

特定のトラフィック カテゴリに属する合計コール数またはコール期間/すべてのカテゴリの合計コール数またはコール期間 * 100。

詳細ビューで、コールの分配の割合を計算するために使用する式は次のとおりです。

1 コール ステータス（失敗、ドロップ、完了、試行）に属するトラフィック タイプの合計コール数/試行コール ステータスに属するトラフィック タイプの合計コール数 * 100。

拠点、コール タイプ、コール ステータス、コール数、通話時間、コール方向、ユーザ ID、またはクラスタに基づいて詳細ビューの詳細をフィルタリングできます。

キャパシティ分析

このダッシュボードは、重要なネットワーク リソースの使用状況の傾向と使用可能なキャパシティを表示します。この情報は、必要に応じて効果的に将来のキャパシティの追加または削減を計画する際に役立ちます。

キャパシティ分析ダッシュボードのすべてのダッシュレットでは、当日のデータが翌日にのみ処理されます。したがって、ダッシュレットには現在の日付のデータをゼロとして表示します。

データ ソース：このダッシュボードの使用率データは、音声使用率のポーリングされたデータから取得されます。

これらのダッシュレットのクイック ビュー、ダッシュレット ビューと詳細ビューでは、フィルタが適用された期間のデータが表示されます。

キャパシティ分析ダッシュボードでサポートされている SIP トランクの詳細は、次の表のとおりです。

SIP トランクのタイプ	% 使用率レポート		煩雑時のトランクのトラフィック レポート	
	データ ソース	サポート	データ ソース	サポート
Cisco CUBE で終端している SIP トランク	CUBE を直接ポーリング	Available	CDR	利用可能
UCM 論理 SIP トランク（ICT、Webex へのトランクなど）	RTMT UCM SIP パフォーマンス カウンタ	該当なし	CDR	利用可能
SIP トランクがシスコ以外のボーダー エレメント（Acme など）で終端	RTMT UCM SIP パフォーマンス カウンタ	該当なし	CDR	利用可能

キャパシティ分析ダッシュボードから、次のダッシュレットを表示できます。

分析グループの管理

Prime Collaboration Analytics では、ビジネス ニーズに基づいてトランク、ルート グループ、およびCAC の拠点に対してカスタム グループを作成することができます。[分析管理（Analytics Administration）] > [グループ管理（Group Management）] をクリックします。右上の [Group Type] ドロップダウンからグループを選択します。新しいグループの作成、既存グループのメンバーの変更、グループの削除を行えます。

たとえば、ネットワーク内のすべてのトランクは [Analytics Group Management] ページに表示されます。トランクを選択し、[All Trunks] でそのトランクを既存のグループに追加（[Add to Group] をクリック）するか、新しいグループに追加（[Add New Group] をクリック）します。

グループを作成すると、使用可能なグループの一覧が左側のペインの [Trunk Groups] に表示されます。これらのグループは、キャパシティ分析ダッシュボードの [All Trunks] ドロップ ダウン（トランク使用率ダッシュレット）にも表示されます。

カスタム ルート グループおよびCAC の拠点を作成するための類似の方法に従うことができます。対応する使用率のしきい値はダッシュレットに表示されます。しきい値を適用すると、結果はしきい値フィルタに基づいてフィルタリングされます。

表示されている列を追加または削除するには、右上の [Settings] アイコンを使用します。

（注）
- MSP モードでは、オペレータ ユーザは [分析管理（Analytics Administration）] メニューにアクセスできないため、カスタム グループを作成することはできません。
- グループ名は追加または削除できますが、編集はできません。
- Analytics Group Management のトランク/ルート グループ、および Prime Collaboration Analytics のその他のダッシュレットは Prime Collaboration Assurance データベースからインポートされますが、Prime Collaboration Analytics で作成されたカスタム グループは Prime Collaboration Assurance では表示、または使用されません。
- 集約されたデータをトランク/ルート グループ使用率ダッシュレットに表示する場合は、[モニタ（Monitor）] > [使用率の監視（Utilization Monitor）] > [ルート グループの使用率（Route Group Utilization）] > [ルート グループの集計設定（Route Group Aggregation Settings）] を使用してカスタム グループを定義する必要があります。
- DSP のカスタム グループを作成する場合は、**[デバイスインベントリ（Device Inventory）] > [インベントリ管理（Inventory Management）] > [グループの作成（Create Group）]**（[デバイスグループ（Device Group）] の下）を使用します。

CAC 帯域幅使用率

この章ではコール アドミッション制御について説明します。コール アドミッション制御は、広域（IP WAN）リンク上で同時にアクティブにするコール数を制限することにより、このリンクを経由するコールの音質およびビデオ品質を制御できます。

非常に多くのアクティブ コールがリンクに存在し、帯域幅の量がオーバーサブスクライブ状態になった場合、音声およびビデオの品質が低下し始める場合があります。コール アドミッション制御は、不十分な帯域幅が存在する場合にコールを拒否し、そのコールを失敗させることで動作します。

拠点名、失敗したコール数（帯域幅の不足によって確立できなかったコール）、および拠点ごとに使用される帯域幅が割合として表示されます。デフォルトでは、テーブルは使用される帯域幅に基づいてソートされます。

ダッシュレットは、ピークおよび音声、ビデオまたはイマーシブとしての使用タイプに基づいてフィルタリングできます。デフォルトでは、帯域幅使用率が、過去 28 日間にピークに達した拠点を表示します。

WAN の場所、使用帯域幅、使用率タイプ、失敗したコール、またはクラスタに基づいて詳細分析に表示される詳細をフィルタリングできます。拠点に基づいてコールをフィルタリングすることもできます。拠点を選択する [Select] オプションを使用します。

このダッシュレットには VCS で処理されたコールの詳細が含まれていません。

トランク使用率

このダッシュレットを使用すると、使用頻度が最も高い、または最も低いトランクを特定できます。このダッシュレットの使用率データは、音声使用率のポーリングされたデータから取得されます。このダッシュレットには、最大同時コール（設定済みのデータ）、同時コール（使用されたデータ）、トランク タイプ、および各トランクの使用率がパーセンテージで表示されます。また、VCS で処理されたコールの詳細も表示されます。

前提条件：

- カスタム トランク グループのデータを表示する場合は、[Analytics Administration] > [Group Management] を使用してこれらのグループを定義する必要があります。
- このダッシュレットに SIP データを入力するには、SIP トランクの最大キャパシティを設定する必要があります。ダッシュレットの左上で、フィルタの下の [Missing Trunk?] をクリックして、SIP の最大キャパシティを設定することができます。

MGCPやクラスタ間などの他のトランクの場合は、ポーリングされたデータを通じてデータが収集されます。

煩雑時のトランク キャパシティ

このダッシュレットを使用すると、Average Bouncing Busy Hour（ABBH）トラフィックが高いトランクを特定できます。ABBH は特定のピリオド（通常 1 週間）の毎日のピーク時にスイッチング システムのトラフィック負荷を分析し、その期間の平均を計算することで算出されます。

前提条件：CDR使用率トランクの最大キャパシティは、このダッシュレットで利用できるキャパシティを確認できるように設定する必要があります。CDR 使用率トランクの最大キャパシティを設定するには、ダッシュレットの左下で、フィルタの下の [煩雑時のトランクがない場合（Missing Busy-Hour Trunk?）] をクリックします。

トランク グループまたはルート グループの次のキャパシティの詳細を表示できます。

- 使用可能なキャパシティ
- 平均 Bouncing Busy Hour トラフィック
- 最大 Bouncing Busy Hour トラフィック

リソースに必要な最大キャパシティは、アーランで表される最大 BBH 値から計算されます。最大 BBH は選択された期間の特定のトランクの最大 Bouncing Busy Hour 値です。BBH は、その日のピーク値です。

必要な平均キャパシティは、ABBH値から計算されます。ここでの平均キャパシティは、優れたトラフィック フローを維持するために必要な最小限のキャパシティを示します。ABBH は選択された期間のトランクまたはルート グループのすべての BBH 値の平均です。

（注） ABBH 値は選択された期間の就業日に限り計算されます。たとえば、期間を 1 週間に指定すると、Analytics は最初に 7 日間の ABBH を計算します。BBH 値が ABBH の 25% 未満になる日は未就業日と見なされます。Analyticsは未就業日を無視し、その週の他のすべての曜日のABBH値を計算します。

デフォルトでは、Analyticsは必要な平均キャパシティおよび必要な最大キャパシティを計算するためにサービス グレード（GOS）の値として 0.01 を使用します。別の GOSのキャパシティ（0.1 や 0.001 など）の必要平均キャパシティと必要最大キャパシティを計算する場合には、root としてサーバに を更新するには、gos. properties ファイルを編集する必要があります。詳細については、「GOS プロパティ ファイルの編集」を参照してください 。

当日の BBH はその日の終わりに計算され、翌日のみ表示できます。ABBH の着信または発信トラフィックはありません。これは BBH だけに適用されます。

トランク、トラフィック タイプ、使用される方向、帯域幅、またはクラスタに基づいて、詳細ビューに表示される詳細をフィルタリングできます（詳細ビューで [Select] オプションを選択した場合のみ、このドロップダウン リストが有効になります）。クラスタを選択するときに、デバイスの使用頻度に関係なくそのクラスタ内のすべてのデバイスが一覧表示されます。

ダッシュレットの利用可能なキャパシティを表示するには、CDR 使用率トランクの最大キャパシティを設定する必要があります。CDR トランクの最大キャパシティが設定されていない場合、またはゼロの場合、これらのトランク データはダッシュレットに反映されません。

このダッシュレットには VCS で処理されたコールの詳細が含まれていません。

アーランの計算

アーランは 1 時間のトラフィックの全体量を説明するために使用されます。たとえばあるグループのユーザが 1 時間に 30 コールを発信した場合は、各コールの通話平均時間は 5 分間となり、アーラン数は以下のように算出されます。

1 時間のトラフィック分数 = コール数 x 通話時間（30*5） = 150

1 時間のトラフィック時間 = 150/60 = 2.5

したがって、トラフィック合計 = 2.5 アーラン。

アーラン トラフィック測定は、音声ネットワーク内のトラフィック パターンを理解するために行われます。また、電話システムとセントラル オフィス（PSTN 交換回線）または複数のネットワーク拠点間の回線数を算出するためにも使用できます。

GOS プロパティ ファイルの編集

Analyticsでは、必要な平均キャパシティおよび必要な最大キャパシティを計算するためにサービス グレード（GOS）の値として 0.01 を使用します。（0.1 や 0.001 などの）別の GOS につい

て必要な平均および最大のキャパシティを計算する場合は、GOS プロパティ ファイルを編集する必要があります。

ステップ 1 管理者権限で Prime Collaboration Assurance サーバにログインします。

ステップ 2 ブラウザで新しいタブを開き、このリンクの URL（https://<pc-server-ip>/emsam/applications/emsam/PCDiagnostics/fileEditor.jsp）を入力します。

ここでの pc-service-ip は Prime Collaboration Assurance サーバの IP アドレスです。

ステップ 3 次のように選択します。

a) [Location] ドロップダウン リストで、[/opt/emms/emsam/advance_reporting/conf/] を選択します。
b) [File Type] ドロップダウン リストで [properties] を選択します。
c) [Files] ドロップダウン リストで [gos.properties] を選択します。

ステップ 4 [Edit] をクリックします。

ステップ 5 gos の値を編集して [Save] をクリックします。

トランクまたはゲートウェイの最大容量の設定

トランクまたはゲートウェイの最大容量を設定するには、次のようにします。

（注） MSP モードでは、オペレータのユーザは [分析管理（Analytics Administration）] メニューにアクセスできないため、トランクまたはゲートウェイの最大容量を設定することはできません。

ステップ 1 **[分析管理（Analytics Administration）] > [トランク トラフィックの最大キャパシティ設定（Trunk Traffic Max Capacity Settings）]** を選択します。

ステップ 2 ドロップダウン リストから、設定する Cisco Unified CM クラスタを選択します。

ステップ 3 ゲートウェイまたはトランクのタイプを選択します。

ステップ 4 [最大キャパシティの設定（Configure Maximum Capacity）] をクリックし、適切な入力を行います。

ステップ 5 [Apply] をクリックして [Close] をクリックします。

すべてのクラスタに関するトランク使用率データのインポート

すべての Cisco Unified CM クラスタのトランク使用率データをインポートするには、次の手順を実行します。

（注） MSP モードでは、オペレータ ユーザは [分析管理（Analytics Administration）] メニューにアクセスできないため、トランクの使用率をインポートすることはできません。

ステップ 1 [分析管理（Analytics Administration）]>[トランクトラフィックの最大キャパシティ設定（Trunk Traffic Max Capacity Settings）] を選択します。

ステップ 2 [Bulk Export] をクリックします。

ステップ 3 [Export Trunk Configuration] ウィンドウで、[Export] をクリックして、デフォルト名のエクスポート CSV ファイルを受け入れます。

ステップ 4 CSV ファイルを開き、必要に応じてデータを編集します。

すべてのゲートウェイおよびトランクがファイルにリストされます。ファイルだけに値を入力する必要があります。

ステップ 5 [Bulk Import] をクリックします。

ステップ 6 CSV ファイルの場所を参照して選択し、[Import] をクリックします。

ルート グループ/トランク グループの使用率

このダッシュレットを使用すると、ルート グループの使用率を追跡できます。

前提条件：

- 集約されたデータを表示するには、ダッシュレットの左上で、フィルタの下の [Missing Route Group/Trunk Group?] をクリックして、トランクをルート グループに関連付ける必要があります。
- ユーザ定義のトランク グループについてデータを表示するには、ダッシュレットの左上で、フィルタの下の [Missing Route Group/Trunk Group?] をクリックしてカスタム グループを作成する必要があります。
- SIP トランクのデータを入力するには、ダッシュレットの左上で、フィルタの下の [Missing Route Group/Trunk Group?] をクリックして SIP トランクの最大キャパシティを設定する必要があります。MGCP やクラスタ間などの他のトランクの場合は、ポーリングされたデータを通じてデータが収集されます。
- カスタム グループのデータを表示する場合は、[Analytics Administration] > [Group Management] を使用してこれらのグループを定義する必要があります。

このダッシュレットには、トランク/ルート グループについて集約されたデータが表示されます。このダッシュレットの使用率データは、音声使用率のポーリングされたデータから取得されます。最大同時コール（設定済みのデータ）、同時コール（使用されたデータ）、および使用率のパーセンテージを表示することができます。ピーク時のルート グループの使用率パターンを、数ヵ月にわたって表示することもできます。

煩雑時のルートグループ キャパシティ

このダッシュレーは、平均的なビジー時間（ABBH）トラフィックが増加しているルート グループを特定するのに役立ちます。ABBH は特定のピリオド（通常 1 週間）の毎日のピーク時

にスイッチング システムのトラフィック負荷を分析し、その期間の平均を計算することで算出されます。

前提条件：CDR使用率トランクの最大キャパシティは、このダッシュレットで利用できるキャパシティを確認できるように設定する必要があります。CDR 使用率トランクの最大キャパシティを設定するには、ダッシュレットの左下で、フィルタの下の [煩雑時のルートグループがない場合（Missing Busy-Hour Route Group?）] をクリックします。

トランク グループまたはルート グループの次のキャパシティの詳細を表示できます。

- 使用可能なキャパシティ
- 平均 Bouncing Busy Hour トラフィック
- 最大 Bouncing Busy Hour トラフィック

リソースに必要な最大キャパシティは、アーランで表される最大 BBH 値から計算されます。最大 BBH は選択された期間の特定のルート グループの最大 Bouncing Busy Hour 値です。BBH は、その日のピーク値です。

必要な平均キャパシティは、ABBH値から計算されます。ここでの平均キャパシティは、優れたトラフィック フローを維持するために必要な最小限のキャパシティを示します。ABBH は選択された期間のルート グループのすべての BBH 値の平均です。

（注） ABBH 値は選択された期間の就業日に限り計算されます。たとえば、期間を 1 週間に指定すると、Analytics は最初に 7 日間の ABBH を計算します。BBH 値が ABBH の 25% 未満になる日は未就業日と見なされます。Analytics は未就業日を無視し、その週の他のすべての曜日の ABBH 値を計算します。

デフォルトでは、Analytics は平均 0.01 は必要平均キャパシティと必要最大キャパシティを計算するために、サービス グレード値として 0.01 を使用します。（0.1 や 0.001 などの）別の GOS について必要な平均および最大のキャパシティを計算するには、 を更新するには、gos.properties ファイルを編集する必要があります。詳細については、「GOS プロパティ ファイルの編集」を参照してください 。

当日の BBH はその日の終わりに計算され、翌日のみ表示できます。ABBH の着信または発信トラフィックはありません。これは BBH だけに適用されます。

詳細分析のページでは、ルート グループ、トラフィック タイプ、方向、使用された帯域幅、またはクラスタに基づいて表示される詳細をフィルタリングできます（このドロップダウン リストは、詳細ビューで [Select] オプションを選択した場合のみ有効です）。クラスタを選択するときに、デバイスの使用頻度に関係なくそのクラスタ内のすべてのデバイスが一覧表示されます。

また、[Show Trunks] を選択すると、ルート グループに関連付けられているトランクのトラフィック タイプおよび方向を表示することができます。（凡例をクリックしたときにポップアップ表示される）表形式のビューには、ルート グループに対して関連付けられているトランクの詳細も表示されます。

ダッシュレットの利用可能なキャパシティを表示するには、CDR 使用率トランクの最大キャパシティを設定する必要があります。CDR トランクの最大キャパシティが設定されていない場合、またはゼロの場合、これらのトランク データはダッシュレットに反映されません。

CDR トランクの最大キャパシティを設定するには、トランクまたはゲートウェイの最大容量の設定 （562 ページ） を参照してください。

このダッシュレットには VCS で処理されたコールの詳細が含まれていません。

DSP 使用率

DSP リソース使用率をトラックして、使用率を最適化することができます。このダッシュレットでは、ゲートウェイの平均および最小の DSP 使用率を表示することができます。

前提条件：このダッシュレットにデータを入力するには、ゲートウェイを検出する必要があります。

クイック ビューで、一定期間における使用率の詳細を表示できます（Gateway列の値にマウスポインタをおくと起動されます）。

詳細な分析のページでは、カスタム グループや DSP 使用率、期間、MTP、トランスコーダ、クラスタ、およびゲートウェイごとにフィルタリングできます。（凡例をクリックするとポップアップ表示される）表形式のビューには、ピーク、平均、および最小の DSP 使用率、時間ごとに使用されるチャネルの合計数が表示されます。

[デバイスインベントリ（Device Inventory）] を使用して、DSP カスタム グループを作成できます。 ページから DSP カスタム グループを作成できます。必要なフィルタ パラメータを適用した後で、[Detailed Analysis] ページで [Save Results] をクリックします。カスタム グループを作成する場合、選択されているゲートウェイの数が 100 を超えていないことを確認する必要があります。カスタム グループは [Device Work Center] ページでのみ編集または削除できます。

（注） **Cisco Prime Collaboration リリース 11.1 以前の場合**

MSP モードでは、オペレータ ユーザにカスタム グループを作成する権限がありません。そのため、[結果の保存（Save Result）] ボタンはグレー表示されます。

サービス エクスペリエンス

このダッシュボードは、コール数、拠点、および通話時間に基づいてサービス品質の分配およびトラフィックの傾向を分析するのに役立ちます。

前提条件：コール測定レコード（CMR）は、平均オピニオン評点（MOS）または Severely Concealed Seconds Ratio（SCSR）の値のいずれかを指定する必要があります。

データ ソース：このダッシュレットのデバイス詳細は、Prime Collaboration インベントリから収集され、このダッシュレットのコール品質の詳細は CDR から取得されます。

詳細分析ビューの他のフィルタだけでなく、サービス エクスペリエンス ダッシュボードの各ダッシュレットでは、（[User] フィールドでユーザ ID を指定して）選択したユーザに基づい

て結果をフィルタすることもできます。表形式のビュー（スライダの下に表示されている凡例/シリーズをクリックするか、またはグラフ上のいずれかの場所をダブルクリックするとポップアップ表示される）にも [User] フィールドがあります。選択したユーザの詳細が含まれている、同じ結果をエクスポートすることもできます。

見つかった問題です。

「コール品質に問題があるユーザ」の [詳細（Detail）] ビュー ページには、「データはありません」と表示されます。

次の操作を実行します。

（注） [クイック（Quick）] ビューに見つかる [詳細（Detail）] ビューページには、データが示しています。

1. ユーザ名「*globaladmin*」とパスワード「*Ecmbu!23*」を使用して、Prime Collaboration Assurance サーバ アドレスの 10.197.94.104 ログインします。
2. 「> サービス エクスペリエンス」に進みます。
3. 「コール品質に問題があるユーザ」ダッシュレットで使用可能なデータを確認します。

   。
4. [詳細の表示（Details）] をクリックします。
5. [詳細（Detail）] ビュー ページには「データなし」と表示されます。

サービス エクスペリエンスの分配

Cisco Prime Collaboration リリース 11.1 以前の場合

このダッシュレットには、次の事前定義されたコール カテゴリに属しているコールの分配の割合が表示されます。

- Good：Severely Concealed Seconds Ratio（SCSR）の値が、ロング コールおよびショート コールの SCSR しきい値より低くなっている。
- Acceptable：SCSR の値が、ロング コールおよびショート コールの SCSR しきい値以上になっている。
- Poor：SCSR の値がロング コールおよびショート コールの SCSR しきい値を超えている。
- Grade Not Available：対応する SCSR の値が有効ではない場合に発生する。

しきい値を設定するには、『Cisco Prime Collaboration Assurance ガイド- Advanced』の「Voice Call Grade Settings の概要」セクションを参照してください。

ダッシュレット ビューでは、表示する図を選択できます。

- 段階別のコール：Good、Acceptable、Poor コール

- 段階別および段階の無いコール：Good、Acceptable、Poor、および Grade Not Available コール

デフォルトでは、ダッシュレット ビューは段階的なコールのグラフを表示します。

コール タイプ、コール品質、デバイス プール、ディレクトリ番号、IP アドレス、URI、クラスタ、または拠点に基づいて、詳細ビューのコール品質のデータをフィルタリングできます。

このダッシュレットのデバイス詳細は、Prime Collaboration インベントリから収集され、このダッシュレットのコール品質の詳細は CDR から取得されます。

このダッシュレットには Cisco Unified Communications Manager で処理されるコールの詳細だけが含まれます。

コール品質の分析

Cisco Prime Collaboration リリース 11.5 以降の場合

このダッシュレットには、次の事前定義されたコール カテゴリに属しているコールの分配の割合が表示されます。

- Good：Severely Concealed Seconds Ratio（SCSR）の値が、ロング コールおよびショート コールの SCSR しきい値より低くなっている。
- Acceptable：SCSR の値が、ロング コールおよびショート コールの SCSR しきい値以上になっている。
- Poor：SCSR の値がロング コールおよびショート コールの SCSR しきい値を超えている。
- Grade Not Available：対応する SCSR の値が有効ではない場合に発生する。

しきい値を設定するには、『Cisco Prime Collaboration Assurance ガイド - Advanced』の「Configuring Global Thresholds」セクションを参照してください。

ダッシュレット ビューでは、表示する図を選択できます。

- 段階別のコール：Good、Acceptable、Poor コール
- 段階別および段階の無いコール：Good、Acceptable、Poor、および Grade Not Available コール

デフォルトでは、ダッシュレット ビューは段階的なコールのグラフを表示します。

コール タイプ、コール品質、デバイス プール、ディレクトリ番号、IP アドレス、URI、クラスタ、または拠点に基づいて、詳細ビューのコール品質のデータをフィルタリングできます。

このダッシュレットのデバイス詳細は、Prime Collaboration インベントリから収集され、このダッシュレットのコール品質の詳細は CDR から取得されます。

このダッシュレットには Cisco Unified Communications Manager で処理されるコールの詳細だけが含まれます。

サービス品質問題があるエンドポイント

Cisco Prime Collaboration リリース 11.1 以前の場合

このダッシュレットは、サービス品質の問題が発生する上位 N のエンドポイント タイプとエンドポイント モデルを一覧表示します。 Cisco DX650、DX70、DX80、88 xx、および 78xx 以外のすべての IP phone の許容品質と低品質コールの傾向を示しています。

このダッシュレットのデバイス詳細は、Prime Collaboration インベントリから収集され、このダッシュレットのコール品質情報は CMR から取得されます。

ダッシュレット ビューで、許容レベルおよび低品質コールの割合の計算に使用する式は次のとおりです。

エンドポイント モデルまたはエンドポイント タイプの低品質および許容レベルコールの合計数/同じエンドポイント モデルまたはエンドポイント タイプ コールの総数 * 100。

詳細ビューで、許容レベルおよび低品質コールの割合の計算に使用する式は次のとおりです。

エンドポイント モデルまたはエンドポイント タイプのコール段階の 1 種類/同じエンドポイント モデルまたはエンドポイント タイプ コールの総数 * 100。

エンドポイント タイプ、エンドポイント モデル、コール タイプ、コール 段階、計算（絶対値または割合）、コール数、通話時間、クラスタ、拠点、デバイス プール、IP アドレス、ディレクトリ番号または URI に基づいて、詳細ビューの詳細をフィルタリングできます。

このダッシュレットには Cisco Unified Communications Manager で処理されるコールの詳細だけが含まれます。

（注） 詳細ビュー グラフに表示されるコール数データは、コール データ レコード テーブルに表示されるデータと同期されません。これは、詳細ビュー グラフがエンドポイント レベルでデータを集約するのに対し（CMR を使用）、コール レコード テーブルはコール詳細レベルでデータを表示するためです（CDR を使用）。

通話品質の問題があるエンドポイント

Cisco Prime Collaboration リリース 11.5 以降の場合

このダッシュレットは、サービス品質の問題が発生している上位 N のエンドポイント タイプおよびエンドポイント モデルを示します。 Cisco DX650、DX70、DX80、88 xx、および 78xx 以外のすべての IP phone の許容品質と低品質コールの傾向を示しています。

このダッシュレットのデバイス詳細は、Prime Collaboration インベントリから収集され、このダッシュレットのコール品質情報は CMR から取得されます。

ダッシュレット ビューで、許容レベルおよび低品質コールの割合の計算に使用する式は次のとおりです。

エンドポイント モデルまたはエンドポイント タイプの低品質および許容レベルコールの合計数/同じエンドポイント モデルまたはエンドポイント タイプ コールの総数 * 100。

詳細ビューで、許容レベルおよび低品質コールの割合の計算に使用する式は次のとおりです。

エンドポイント モデルまたはエンドポイント タイプのコール段階の 1 種類/同じエンドポイント モデルまたはエンドポイント タイプ コールの総数 * 100。

エンドポイント タイプ、エンドポイント モデル、コール タイプ、コール 段階、計算（絶対値または割合）、コール数、通話時間、クラスタ、拠点、デバイス プール、IP アドレス、ディレクトリ番号または URI に基づいて、詳細ビューの詳細をフィルタリングできます。

このダッシュレットには Cisco Unified Communications Manager で処理されるコールの詳細だけが含まれます。

（注） 詳細ビュー グラフに表示されるコール数データは、コール データ レコード テーブルに表示されるデータと同期されません。これは、詳細ビュー グラフがエンドポイント レベルでデータを集約するのに対し（CMR を使用）、コール レコード テーブルはコール詳細レベルでデータを表示するためです（CDR を使用）。

上位 N のコール失敗発生拠点

Cisco Prime Collaboration リリース 11.1 以前の場合

このダッシュレットは、失敗したコール数が最も高い（帯域幅の不足によって確立しなかったコール）上位 N の拠点を表示します。

このダッシュレットは、失敗したコール数が最も高い（帯域幅の不足によって確立しなかったコール）拠点を表示します。各エンドポイントでコールが正常にクリアされた段階でコールは良好と見なされます。

このダッシュレットの拠点情報は CDR から収集します。

拠点、コール タイプ、コール ステータス、コール数、通話時間、コール方向、またはクラスタに基づいて詳細ビューの詳細をフィルタリングできます。

詳細ビューに、ユーザが選択した原因コードをまとめた原因コード分析レポートを表示できます。円グラフの 1 区画が 1 つの原因コードに対応します。グラフで原因コードの出現数と割合を参照するには、カーソルを円グラフの 1 つの区画に移動します。

ダッシュレット ビューでは、失敗したコールの割合を計算するために使用する式は次のとおりです。

拠点で失敗したコールの総数/同じロケーションでの合計コール数 * 100

このダッシュレットには Cisco Unified Communications Manager で処理されるコールの詳細だけが含まれます。

詳細ビューでは、失敗したコールの割合を計算するために使用する式は次のとおりです。

コール数または特定のコール ステータスのコール通話時間（失敗、ドロップ、完了、試行）/同じ場所、コール タイプ、コール方向のコール数または通話時間 * 100

失敗したコールの原因コードについては、『Cisco Unified Communications Manager Call Details Record Administration Guide』の「**Call termination cause codes**」を参照してください。

場所のコール ステータス

Cisco Prime Collaboration リリース 11.5 以降の場合

このダッシュレットは、失敗したコール数が最も高い（帯域幅の不足によって確立しなかったコール）拠点を表示します。各エンドポイントでコールが正常にクリアされた段階でコールは良好と見なされます。

このダッシュレットの拠点情報は CDR から収集します。

拠点、コール タイプ、コール ステータス、コール数、通話時間、コール方向、またはクラスタに基づいて詳細ビューの詳細をフィルタリングできます。

詳細ビューに、ユーザが選択した原因コードをまとめた原因コード分析レポートを表示できます。円グラフの 1 区画が 1 つの原因コードに対応します。グラフで原因コードの出現数と割合を参照するには、カーソルを円グラフの 1 つの区画に移動します。

ダッシュレット ビューでは、失敗したコールの割合を計算するために使用する式は次のとおりです。

拠点で失敗したコールの総数/同じロケーションでの合計コール数 * 100

このダッシュレットには Cisco Unified Communications Manager で処理されるコールの詳細だけが含まれます。

詳細ビューでは、失敗したコールの割合を計算するために使用する式は次のとおりです。

コール数または特定のコール ステータスのコール通話時間（失敗、ドロップ、完了、試行）/同じ場所、コール タイプ、コール方向のコール数または通話時間 * 100

失敗したコールの原因コードについては、『Cisco Unified Communications Manager Call Details Record Administration Guide』の「**Call termination cause codes**」を参照してください。

サービス品質問題があるユーザ

Cisco Prime Collaboration リリース 11.1 以前の場合

このダッシュレットには、サービス品質に問題のあるユーザが表示されます。これは、ユーザの音声およびビデオのコール品質について、許容レベルおよび低品質なコールの傾向を示します。

詳細ビューでは、コール タイプ（音声またはビデオ）、コール グレード（良い、許容レベル、低品質）、計算（絶対値またはパーセンテージ）、コール件数、コール期間、クラスタ、拠点、デバイス プール、エンドポイントの IP アドレス、およびユーザに基づいてフィルタリングすることができます。

コール品質に問題があるユーザ

Cisco Prime Collaboration リリース 11.5 以降の場合

このダッシュレットには、サービス品質に問題のあるユーザが表示されます。これは、ユーザの音声およびビデオのコール品質について、許容レベルおよび低品質なコールの傾向を示します。

詳細ビューでは、コールタイプ（音声またはビデオ）、コールグレード（良い、許容レベル、低品質）、計算（絶対値またはパーセンテージ）、コール件数、コール期間、クラスタ、拠点、デバイス プール、エンドポイントの IP アドレス、およびユーザに基づいてフィルタリングすることができます。

Call Grade for Locations

Cisco Prime Collaboration リリース 11.5 以降の場合

このダッシュレットには、場所に基づき、不良、許容可能、良好なコールの合計数が一覧表示されます。また、全体的なコールエクスペリエンスを提供するため、不良なコールは赤色、許容可能なコールはオレンジ、良好なコールは緑色、グレードできないものは黄色で表示されます。

このダッシュレットの拠点情報は CDR から収集します。

コール グレードの詳細情報を表示するには、ダッシュレットの右下隅に表示される **[詳細の表示（See Details）]** をクリックします。**[詳細分析（Detailed Analysis）]**ページでは、通話の種類、通話品質、通話数、通話時間、計算（絶対またはパーセント）、デバイス プール、クラスタ、場所、個別またはマージされたグラフに基づき、コール グレードをフィルタリングできます。

詳細ビューでは、パーセンテージの計算には次の数式を使用します。

特定のコール グレードのコール合計数 (良好、許容可能、不良、またはグレードなし) / コールの合計数（良好 + 許容可能 + 不良 + グレードなし) * 100

Cisco Prime Collaboration リリース 11.1 以前の場合

また、**[詳細分析（Detailed Analysis）]** ページではしきい値の範囲を設定して、不良、許容可能、良好なコールを設定することもできます。コール グレードのしきい値を設定するには、**[詳細分析（Detailed Analysis）** ページの **[設定（configure）]** をクリックします。コール グレードしきい値の設定の詳細については、『Cisco Prime Collaboration Assurance ガイド - Advanced』の「[Voice Call Grade Settings」セクションを参照してください。

ビデオ会議

Cisco Prime Collaboration リリース 11.1 以前の場合

このダッシュボードには、会議リソースの使用状況の傾向が表示されます。この情報は、必要に応じて効果的に将来のキャパシティの追加または削減を計画する際に役立ちます。

前提条件：ダッシュボードのデータは、会議に少なくとも 2 つのビデオエンドポイント（多目的、イマーシブ、またはパーソナル テレプレゼンス）がある場合のみ取り込まれます。

このダッシュボードは、拠点について、会議の最大数、会議の時間（分単位）、および参加者数を表示します。これらのダッシュレットのクイック ビュー、ダッシュレット ビュー、および詳細ビューには、選択した期間のデータが表示されます。

会議ダッシュボードから次のダッシュレットを表示できます。

ビデオ会議の分析

Cisco Prime Collaboration リリース 11.5 以降の場合

このダッシュボードには、会議リソースの使用状況の傾向が表示されます。この情報は、必要に応じて効果的に将来のキャパシティの追加または削減を計画する際に役立ちます。

前提条件：ダッシュボードのデータは、会議に少なくとも2つのビデオエンドポイント（多目的、イマーシブ、またはパーソナル テレプレゼンス）がある場合のみ取り込まれます。

このダッシュボードは、拠点について、会議の最大数、会議の時間（分単位）、および参加者数を表示します。これらのダッシュレットのクイック ビュー、ダッシュレット ビュー、および詳細ビューには、選択した期間のデータが表示されます。

会議ダッシュボードから次のダッシュレットを表示できます。

ビデオ会議の統計情報

コール タイプとコール カテゴリに基づいて、サイト内の会議コールを分析することができます。

このダッシュレットには、コール タイプ（アドホック、スケジュール済み）、およびコール カテゴリ（p2p、マルチサイト、マルチポイント）に基づいて参加者数、会議の件数、および期間が表示されます。

詳細ビューでは、会議タイプと会議のカテゴリについて会議、参加者、および期間に基づいてフィルタリングできます。会議あたりの参加者数、および会議あたりの期間に基づいて表示をカスタマイズできます。

（注） MSPモードでは、アドホック、スケジュール、すべてのフィルタに基づき、ダッシュレットの詳細をフィルタすることはできません。

Cisco Prime Collaboration リリース 12.1 SP2 以降の場合

ビデオ会議統計の前提条件

（注） Conference Diagnostics を有効にしてデータが入力できることを確認します。

ビデオ会議統計の要件は、次のとおりです。

- Unified CM および Cisco VCS は、Managed 状態にある必要があります。

- MCU などのエンドポイントとコントローラは、Managed 状態にある必要があります。
- デバイスの可視性を 「Full Visibility」 状態に設定します。
- JTAPI が Unified Communications Manager で設定されている必要があります。Unified Communications Manager で JTAPI を有効にする方法については、「Cisco Prime Collaboration Assurance のデバイス設定」を参照してください。
- Cisco Prime Collaboration Assurance サーバが、Cisco VCS でフィードバック サーバとして登録されている必要があります。
- 会議の診断と音声電話機能の模擬テストを正しく実行するには、Cisco Prime Collaboration Assurance Service Pack 1 バンドルを適用する前に、CUCM がリストされているバージョンであることを確認してください。詳細については、12.1 Service Pack 1 の『Cisco Prime Collaboration Assurance でサポートされているデバイス』を参照してください。

上位 N のビデオ会議の拠点

を選択できます。拠点ごとに、会議コールおよび会議期間全体における参加者の数を分析できます。コール タイプ（アドホックとスケジュール済み）、コール カテゴリ（p2p、マルチサイト、マルチポイント）のデータをフィルタリングできます。

詳細ビューでは、会議の数が最大または最小の拠点に基づいてフィルタリングできます。会議のタイプ（アドホック、スケジュール済み）、セッション タイプ（P2P、マルチポイント、マルチサイト）、および拠点内のクラスタについて詳細を表示できます。

クラスタ フィルタは、Cisco VCS をサポートしていません。

（注） MSP モードでは、アドホック、スケジュール、すべてのフィルタに基づき、ダッシュレットの詳細をフィルタすることはできません。

Cisco Prime Collaboration リリース 12.1 SP2 以降の場合

Top N Video Conference Locations の前提条件

（注） Conference Diagnostics を有効にしてデータが入力できることを確認します。

Top N video Conference Locations の要件は、次のとおりです。

- Unified CM および Cisco VCS は、Managed 状態にある必要があります。
- MCU などのエンドポイントとコントローラは、Managed 状態にある必要があります。
- デバイスの可視性を 「Full Visibility」 状態に設定します。

- JTAPI が Unified Communications Manager で設定されている必要があります。Unified Communications Manager で JTAPI を有効にする方法については、「Cisco Prime Collaboration Assurance のデバイス設定」を参照してください。
- Cisco Prime Collaboration Assurance サーバが、Cisco VCS でフィードバック サーバとして登録されている必要があります。
- 会議の診断と音声電話機能の模擬テストを正しく実行するには、Cisco Prime Collaboration Assurance Service Pack 1 バンドルを適用する前に、CUCM がリストされているバージョンであることを確認してください。詳細については、12.1 Service Pack 1 の『Cisco Prime Collaboration Assurance でサポートされているデバイス』を参照してください。

会議用デバイスのビデオ使用率

このダッシュレットは、および使用されている会議デバイスの追跡に役立ちます。

前提条件：会議ブリッジが Device Work Center に導入され、検出されていること。

また、

- 特定の期間における会議デバイスのビデオ ポートのピークおよび平均使用統計情報を提供します。
- ネットワーク内に設定されているビデオ ポートの使用率の傾向を調べ、管理の向上に役立ちます。 デバイスに設定されているビデオ ポートの最大数、および使用しているポート数について情報を提供します。

詳細は、会議デバイス、使用率、ピークまたは平均ポート、使用割合、デバイス タイプ（Multipoint Control Unit（MCU）、Cisco TelePresence Multipoint Switch（CTMS）、TelePresence Server（TPS）など）に基づき、絞り込むことができます。それぞれのデバイス タイプに対して Conductor およびデバイス情報を選択することも可能です（詳細ビューで [Select] オプションを選択した場合のみ、これらのドロップダウン リストが有効になります）。

ピークおよび平均のポート使用率フィルタのみが、ダッシュレット、詳細ビュー、クイック ビューに適用されます。

Conductor Bridge Pool の使用率

Cisco Prime Collaboration リリース 11.5 以降の場合

このダッシュレットには、ネットワーク内のコンダクタ プールごとに会議ブリッジの累積使用状況が表示されます。

ダッシュレットには、次の詳細が表示されます。

- [プール名（Pool Name）]：会議ブリッジ プールの名前
- [ビデオポート/スクリーンライセンスの使用状況（Video Ports/Screen License Utilization）]：現在使用中のビデオ ポート/スクリーン ライセンスの数
- [ビデオポート/スクリーンライセンスの最大使用状況（Max Video Ports/Screen License Utilization）]：使用可能なビデオ ポート/スクリーン ライセンスの数。

- [使用率（Utilization）]：使用可能な最大ビデオ ポートの数に対する、使用されたビデオ ポートのパーセンテージ。
- Conference Bridge Type
- [コンダクタ名（Conductor Name）]：会議ブリッジ プールを管理しているコンダクタの名前。

使用状況タイプ（ピークや平均など）および使用率（%）に基づいて、データをフィルタ処理できます。

また、[詳細の表示（See Details）] リンクをクリックすると、デバイスの詳細情報を確認できます。詳細ビューでは、すべてのデバイスまたは選択したデバイスの詳細を、デバイス タイプ、デバイス、期間、使用状況のピークまたは平均、使用率（%）、個別またはマージされたグラフに基づいてフィルタ処理することができます。

UC システム パフォーマンス

このダッシュボードを使用すると、UCアプリケーションのCPUとメモリに基づいてシステムパフォーマンスを分析できます。これらの傾向を使用して、一定期間に常に多量の CPU/メモリを使用している UC アプリケーションを特定することができます。

前提条件：Unified CM および Cisco VCS に登録されているエンドポイントが検出されていること。

データ ソース：このダッシュボードのパフォーマンス使用率の詳細は、RTMT のポーリングされたデータから取得されます

これらのダッシュレットのクイック ビュー、ダッシュレット ビューと詳細ビューでは、フィルタが適用された期間のデータが表示されます。

次のダッシュレットを使用できます。

CPU 使用率：このダッシュレットには、各デバイスのピーク、平均、および最小の使用率について CPU 使用率データが（パーセンテージとして）表示されます。

メモリ使用率：このダッシュレットには、メモリの合計量および使用量（ピーク、平均、最小）がMB単位で表示されます。また、メモリ使用率のピーク、平均、最小についてパーセンテージで表示されます。

（注）
- これらのダッシュレットには、同時に最大 25 行が表示されます。
- また、過去2日間のスパークラインの傾向としてデータ（ピーク、平均、最小）が表示されます。

ライセンスの使用状況（License Usage）

このダッシュボードは、Unified Contact Center Enterprise（UCCE）や Cisco Voice Portal（CVP）などのアプリケーションのライセンス使用状況の追跡をサポートします。

前提条件：ライセンスの使用状況ダッシュボードにデータを入力するには、Contact Center Assurance License が必要です。

データ ソース：このダッシュボードのライセンス使用状況の詳細は、音声使用率のポーリングされたデータから取得されます。

ライセンスの使用状況ダッシュボードでは、次のダッシュレットを使用できます。

Contact Center Enterprise

このダッシュレットには、Unified Contact Center Enterprise のライセンス使用状況が表示されます。

ダッシュレットには、次の詳細が表示されます。

- デバイス：デバイス名
- 機能：ルータやペリフェラル ゲートウェイなどのデバイスの機能
- インスタンス名：インスタンスの名前
- ログオン中のエージェント：現在ログオンしているコンタクトセンターのエージェントの数

ピークや平均などの使用率タイプに基づいて、データをフィルタできます。デフォルトでは、ダッシュレットに過去 14 日間のピークの使用率とデバイスの一覧が表示されます。

デバイスのクイック ビューを起動するには、各デバイス名について使用できる情報アイコンをクリックします。クイック ビューには、一定期間にログオンしたエージェントの数がグラフまたはグリッド ビューの形式で表示されます。

また、[詳細の表示（See Details）] リンクをクリックすると、デバイスの詳細情報を確認できます。詳細ビューで、期間、クラスタ、機能、デバイス、ピークまたは平均の使用率、個別またはマージされたグラフに基づいて、すべてのデバイスまたは選択したデバイスの詳細をフィルタリングすることができます。

顧客音声ポータル

このダッシュレットには、CVP コール サーバのライセンス使用率が表示されます。

このダッシュレットに表示される詳細は次のとおりです。

- デバイス：デバイス名です。
- **Cisco Prime Collaboration リリース 11.1 以前の場合**

  タイプ：デバイス タイプです。集約されたデバイスの場合、デバイス タイプは「マルチデバイス」になります。

Cisco Prime Collaboration リリース 11.5 以降の場合

タイプ：デバイス タイプです。集約されたデバイスの場合、デバイス タイプは「デバイス グループ（Device Group）」になります。

- 使用中のポート：現在使用されているポート ライセンスの数です。
- ポートの最大数：新しいコールの処理で使用できるポート ライセンスの数です。選択した期間に使用されたポートで何らかの変更があった場合は、利用できる最小から最大のポート範囲が表示されます。
- 使用率（%）：利用可能な最大ポートで使用されたポートの使用率。
- ポート要求の拒否：システムの開始以後に拒絶されたポート ライセンス チェックアウト要求の数。

Cisco Prime Collaboration リリース 11.5 以降の場合

複数のデバイスの集約されたライセンス使用状況を確認できます。集約されたデバイスの場合は、「集約デバイス」を参照してください。

ピークや平均などの使用率タイプに基づいて、データをフィルタできます。デフォルトでは、ダッシュレットに過去 14 日間のピークの使用率とデバイスの一覧が表示されます。

デバイスのクイック ビューを起動するには、それぞれのデバイスで使用できる情報アイコンをクリックします。クイック ビューには、使用中のポート、およびそのポートの特定期間での使用率がグラフまたはグリッド ビューで表示されます。

[See Details] リンクをクリックすると、デバイスの詳細情報を表示することもできます。詳細ビューでは、すべてのデバイス、特定の期間に基づいて選択または集約されたデバイス、使用率の範囲、クラスタ、デバイス、ピークまたは平均の使用率、パーセンテージまたは絶対値、個別またはマージされたグラフで詳細をフィルタできます。

集約デバイス

Cisco Prime Collaboration リリース 11.5 以降の場合

複数の CVP デバイスを選択し、これらのデバイスの集約されたライセンス使用状況を表示することができます。

（注） このタスクを実行するには、管理者特権が必要です。

集約するデバイスを選択するには、次のようにします。

ステップ 1 [Customer Voice Portal（Customer Voice Portal）] ダッシュレットの左上隅にある [CVP集約の設定（CVP Aggregation Configuration）] をクリックします。

ステップ 2 [CVP集約の設定（CVP Aggregation Configuration）] ページで、導入したモードに基づいて、次の操作を実行します。

- Enterprise モードでは、必要に応じて集約用のデバイスを選択します。

- MSP モードでは、次のように個々の顧客のデバイスを集約できます。
  1. 顧客名をクリックします。顧客に関連付けられているデバイスが表示されます。
  2. 表示されたデバイスから、集約に必要なデバイスを選択します。
  3. 集約されたデバイスの名前を入力します。

ステップ 3 [Save] をクリックします。

[Customer Voice Portal（Customer Voice Portal）] ダッシュレットで入力される、デバイス タイプが [デバイスグループ（Device Group）] である集約されたデバイスの値を確認できます。

マイ ダッシュボード

[My Dashboard] ページでダッシュボードをカスタマイズして、既存のダッシュレットを追加することができます。

また、次の操作を実行できます。

- 新しいダッシュボードを作成する。
- 既存のダッシュレットを追加する。
- ダッシュレットをドラッグアンドドロップして、ダッシュボードの下に移動する。
- ダッシュレットを編集および削除する。
- グローバル フィルタを追加する。
- レイアウト テンプレートを変更する。デフォルトでは、[My Dashboard] のレイアウト テンプレートは 100 に設定されています。

新規ダッシュボードを追加するには、次の手順を実行します。

ステップ 1 [My Dashboard] ページの右上の [Settings] アイコンをクリックし、[Add New Dashboard] をクリックします。

ステップ 2 表示されるテキストボックスに名前を入力して [Apply] をクリックします。

ステップ 3 [Add Dashlet(s)] をクリックします。

ステップ 4 追加するダッシュレットの隣の [Add] をクリックします。

カスタム レポート

Prime Collaboration Analytics のカスタム レポートは OLAP のキューブ技術に基づいています。レポートを選択する場合には、分析レポートを生成するために必要な属性と値を柔軟に選択することができます。

属性には、DialledNumber、Date、Time、Cluster、MeetingCategory などの要素が含まれており、数値として表示される値には件数や期間などが含まれています。分析キューブの属性と値の詳細については、『Prime Collaboration Analytics Custom Report』の「Attributes and Values」のページを参照してください。

以下の内容について、Analytics のカスタム レポートを生成できます。

コール品質

- 発信者および着信者の通話状況。発信側または宛先のエンドポイントについて切断、失敗などの通話状況を表示します。
- 発信者および着信者のコール グレード。発信側または宛先のエンドポイントについて、No MOS、低コール、ショート コールなどのコール品質を表示します。発信側または宛先の EP について、（CMR レコードを使用して）コール グレードの詳細も表示します。
- 発信者および着信者のコール クラス。発信側またはエンドポイントの情報について外部、内部、会議などのコールのトラフィック タイプを表示します。また、オンネットとオフネット コールのインジケータを示します。
- 発信および着信者のコールの原因コード。発信側および宛先のエンドポイント情報について、コールの終了コード（一時的な障害（41）、宛先での不具合（27）、ユーザの応答なし（18）など）を表示します。

キャパシティ プランニング

- 拠点の CAC 帯域幅使用率：CAC の帯域幅使用率の詳細、および帯域幅不足で失敗したコールの数が表示されます。
- 会議デバイスのビデオ使用率：Cisco MCU、Cisco TPS などの会議用デバイスについてチャネルの使用率を表示します。
- 煩雑時のトランク キャパシティ：Unified CM CDR から収集された ABBH（Average Bouncing Busy Hour）データを表示します。
- 使用率：トランク、DSP、MTP/Transcoder、ルート グループ、およびトランク グループ。

会議

- 会議の拠点：会議の詳細（エンドポイントについての会議のカテゴリや件数など）を表示します。
- 会議の統計情報：会議の詳細（参加者の人数や期間など）を表示します。

システム パフォーマンス

CPU およびメモリの使用率。

カスタム レポートの作成

カスタム レポートを作成するには、次の手順を実行します。

ステップ 1 選択 **[診断（Analyze）]** > **[カスタム レポート ジェネレータ（Custom Report Generator）]**。

ステップ 2 [Reports] ドロップダウン リストからレポートを選択します。

ステップ 3 [Attributes] ペインと [Values] ペインから要素を選択します。

[Attributes] 要素をダブルクリックし、必要なパラメータを表示して選択します。

[Attributes] の要素は階層、つまり一連の親子関係として編成し、親メンバーはそれぞれの子をまとめることができます。ある親要素は、別の親の子として集約することもできます。たとえば「2014 年 5 月」の親は「2014 年第二四半期」ですが、これは「2014 年」の子となります。

カスタム レポートに関連するネットワーク分析またはUC の使用率では、13 ヵ月を超えて時間データの表示を選択した場合に、レポートの生成に時間がかかることがあります。時間データの対象期間は、13 ヵ月未満にすることを推奨しています。

ステップ 4 **[Save（保存）]** をクリックします。

（注） カスタム レポート ジェネレーターは、MSP モードではサポートされていません。

生成したレポートは、チャートまたはグリッド モードで表示することができます。レポートは、表示モードに基づいて PDF、MS Excel、PNG などでエクスポートすることができます。

定義済みのクエリについては、該当するクエリをMDX言語で表示することができます。MDX は、OLAP キューブに対して問い合わせを行うための言語です。MDX は SQL に似ていますが、キューブの多次元特性のサポートが追加されています。MDX クエリの詳細については、「Mondrian Documentation」を参照してください。MDX クエリを記述する場合には、レポートを生成するための属性と値を使用する必要があります。「Attributes and Values」のページを参照してください。

スケジュール済みレポート

このダッシュボードには、スケジュールが設定されているエンティティ（レポート）の一覧が表示されます（ダッシュレットの左下のドロップダウンで**[Schedule Report]** をクリックします）。このダッシュレットを表示するには、を選択します。**[分析（Analytics）]**> **[スケジュール済みレポート（Scheduled Reports）]**。

レポート名、レポートのタイプ、スケジュールの頻度、スケジュール設定時に使用したフィルタ（ダッシュレットの左下のドロップダウンから **[Schedule Report]** をクリックしたときに **[Filter Settings]** に表示される）、レポートが最後に生成されたときに成功/失敗を示すステータス、および次にスケジュールされている実行のタイミングを確認できます。

上部のメトリックパネルには、ディスク使用率のデータ、電子メールで送信されるレポート、および SFTP サーバへエクスポートされるレポートが表示されます。

ジョブは一時停止することも、再開することもできます（ジョブを選択して [Suspend] または [Resume] をクリックします）。エラーの場合は、ジョブの上にマウスをおいてエラーを表示してください。

ビジネスニーズに基づいて、表示する列を追加、または削除できます。これには、ページの右上にある **[Settings]** アイコンをクリックして、**[Columns]** にマウスをおきます。

レポートをすぐに生成するには、次のようにします。

- （各レポートが表示されている行の最後で）[Run Now] をクリックします。
- [すぐに実行（Run Now）] の隣にある [実行履歴（Run History）] をクリックすると、レポートを実行した回数が表示されますが、一覧表示されるファイル数は過去 30/35 日間に限定されます。実行されたレポートのリストが表示されます。
- レポートをダウンロードすることも、選択したレポートを消去することもできます。

（注）
- スケジュール期間が過ぎた（終了日に達した）レポートでは [Run Now] を使用できません。
- [Run Now] をクリックしても、そのジョブの元のスケジュール（毎日、毎週など）は変更されません。

Cisco Prime Collaboration リリース 11.6 以降の場合

Concurrent Hourly レポート（Top N Call Traffic Locations）：

1. PCA を起動します。
2. [アナリティクス（Analytics）] をクリックします。
3. ドロップダウン リストから [トラフィック分析（Traffic Analysis）] をクリックします。
4. 'Top N Call Traffic Locations' ダッシュレットの右下にある [詳細の表示（See Details）] をクリックすると、[詳細分析（Detailed Analysis）] ページが表示されます。
5. [エクスポート（Export）]、[スケジュール済みエクスポート（Scheduled Export）] の順にクリックし、[スケジュール済みレポート（Scheduled Reports）] のダイアログ ボックスを生成します。
6. **[ここにチェックを入れて前日のレポートをスケジュールする（check this to Schedule hourly reports for previous day）]** ボックスをオンにし、[フィルタ設定（Filter Settings）] の下にある [スケジュール済みレポート（Scheduled Reports）] ダイアログ ボックスの下で Concurrent Hourly Scheduled レポートを生成します。

   [Concurrent Call Hourly] チェックボックスをオンにしないと、フィルタ内の「期間」は変わらないため、生成された PDF に時間データは含まれません。

Top N ロケーション ダッシュレットでは、間隔を 1 日に選択すると、スケジュール設定されたレポート（PDF）は「棒グラフ」の形で生成されます。グリッド/テーブルには、時間/日単位の Concurrent データがあります。Top N ロケーション ダッシュレットから生成された同じ PDF レポートには、棒グラフ/グリッドがともに表示されます。

Daily Report（上位 N 番の発信者と上位 N 個のダイヤルされた番号）：

1. PCA を起動します。
2. [アナリティクス（Analytics）] をクリックします。
3. ドロップダウン リストから [トラフィック分析（Traffic Analysis）] をクリックします。
4. [Top N callers/Top N Dialed Numbers] ダッシュレットで、上位 N 番の発信者と上位 N 個のダイヤルされた番号のダッシュレットの下にある [↗（曲がった右矢印）] をクリックします。
5. ドロップダウン メニューから [スケジュール済みレポート（Scheduled Reports）] をクリックし、[スケジュール済みレポート（Scheduled Report）] ウィンドウを表示します。
6. 日次レポートを表示するには、[ここをチェックして日次レポートをスケジュールする（Check this to schedule daily report）] チェックボックスをオンにします。

   スケジュール済みレポートのフィルタで変更されたタイトルや時間を表示するには、このチェックボックスをオンにします。

Prime Collaboration Analytics ダッシュボードのトラブルシューティング

次の表に、個々のダッシュボードにおけるデータ入力のトラブルシューティングの詳細が記載されています。

表 *67 :* 個々のダッシュボードのトラブルシューティングの詳細

ダッシュボード	前提条件	データ ソース	関連付けられた レポートでデータの収集を確認
資産使用状況	エンドポイントが検出されている必要がある。	CDR および Prime Collaboration インベントリ	
トラフィック分析		CDR	

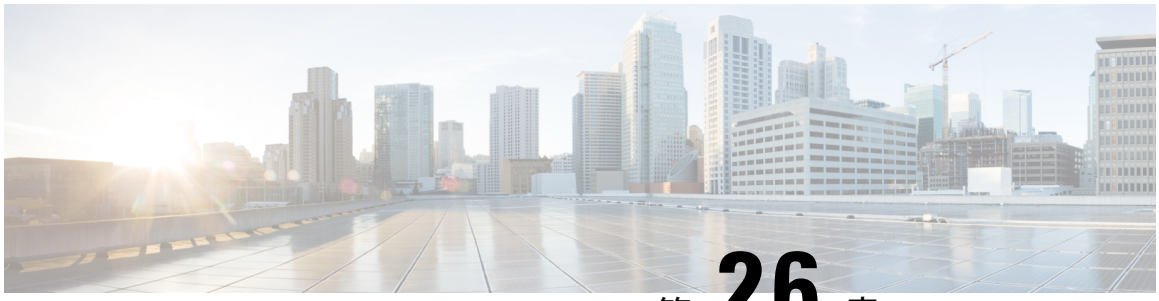
キャパシティ分析	• **トランク使用率**：SIP トランクの最大キャパシティを設定して、カスタム トランク グループを定義する。 • **煩雑時のトランクおよび煩雑時のルート グループ最繁時のルートグループ キャパシティ**： CDR トランクの最大キャパシティを設定する必要がある。 • **ルートグループ/トランクグループの使用率**：SIP トランクの最大キャパシティを設定し、カスタム トランク グループを定義してトランクをルート グループに関連付ける。 • **会議デバイス ビデオの使用率**：会議ブリッジが Device Work Center で導入および検出され、これらのメディア リソース（MCU、TPS、CTMS）のいずれかからのコールが存在する必要がある。 • **DSP 使用率**：ゲートウェイが検出されている必要がある。	音声使用率のポーリングされたデータ	**[監視（Monitor）] > [使用率の監視（Utilization Monitor）]**
サービス エクスペリエンス	CMR が MOS および SCSR グレードの詳細を提供している必要がある。	CDR および Prime Collaboration インベントリ	**[ネットワーク正常性の概要（Network Health Overview）] > [サービス エクスペリエンス（Service Experience）]**

Cisco Prime Collaboration リリース 11.1 以前の場合 ビデオ会議 **Cisco Prime Collaboration リリース 11.5 以降の場合** ビデオ会議の分析	• 会議で少なくとも 2 つのビデオ エンドポイントが使用可能である必要がある。 • **ビデオ会議の統計**： エンドポイントの可視性を [Full] または（**[インベントリ（Inventory）] > （[現在のインベントリ（Current Inventory）] の下から [編集（Edit）]**）に設定し、セッションの詳細をポーリングする必要があります。		**[診断（Diagnose）] > [会議の診断（Conference Diagnostics）]**

第 VIII 部

診断の実行

- 音声エンドポイントの診断 （587 ページ）
- ビデオ エンドポイントのトラブルシューティング ワークフロー （657 ページ）
- メディア パスの分析 （681 ページ）
- ログの収集 （685 ページ）
- コール シグナリングの分析 （693 ページ）



第 26 章

音声エンドポイントの診断

このセクションでは、次の点について説明します。

- 音声エンドポイントの診断 （587 ページ）

音声エンドポイントの診断

Cisco Prime Collaboration Assurance では、複数の診断テストを実行して Unified Communications 電話ネットワークに関する問題を特定できます。

Cisco Prime Collaboration Assurance を MSP モードで導入した場合は、テスト結果を表示する顧客を選択することができます。ユーザインターフェイスの右上にあるグローバル顧客選択リストを使用して、顧客を選択してからテストを実行します。テストを実行するために使用可能なエンドポイントは、選択した顧客によって異なります。テスト結果には、デバイスが属している顧客が表示されます。テストのフィールドを作成、インポート、スケジューリング、変更した後にグローバル顧客選択リストから顧客を選択または選択解除した場合、その変更の結果はページが更新されたときに表示されます。

音声エンドポイントの次の診断テストを実行できます。

Phone Status Test

電話ステータス テストでは Cisco IOS IP SLA テクノロジを使用し、ネットワーク内の主要電話機の到達可能性を監視します。電話ステータステストはプロトコルに依存しません。これらのプロトコル、SCCP、SIP で動作する電話機をテストできます。電話ステータス テストは、次の内容で構成されます。

- ユーザが選択したテスト対象 IP 電話のリスト。
- ユーザが設定したテスト スケジュール。
- IP フォンに対して IP SLA 対応デバイス（スイッチ、ルータ、または音声ルータなど）から IP SLA ベースの ping。また、オプションとして、Cisco Prime Collaboration Assurance から IP phone に ping することもできます。

電話機は、IP SLA ベースの ping、または Cisco Prime Collaboration Assurance の ping に応答しない場合は到達不可能と見なされ、電話ステータスは、電話ステータス プロセスで登録解除と表示されます。Cisco Prime Collaboration Assurance は PhoneReachabilityTestFailed イベントを生成します。

ルータがリブートされた場合、電話ステータス テストは失われます。ただし、Cisco Prime Collaboration Assurance は、ルータが利用可能になるとテストを再設定します。ルータがダウンになったとしても、Cisco Prime Collaboration Assurance の ping が有効な場合、Cisco Prime Collaboration Assurance は引き続き ping を実行します。

電話ステータス テストは、電話機情報（IP アドレスや内線番号）が変更、ならびに電話機関連のデバイスが Cisco Prime Collaboration Assurance によって監視されていない場合を除いては引き続き実行され、シード ファイルを更新し、テストを再追加します。

[Create Phone Status Test] ページを使用するか、シード ファイルを使用して、電話ステータス テストを作成できます。最新の Cisco Unified CM に最も近くの場所にある IP SLA 対応デバイスでテストを設定する場合は、シードファイルを更新し、テストを再追加します。

（注） Cisco Prime Collaboration Assurance をアンインストールする前には、必ずアプリケーションからすべての電話ステータステストを削除します。これらのテストを削除しないと、ルータでテストの実行が続行されます。

SNMP V3 クレデンシャルを使用して IP SLA 対応デバイスを管理した場合は、CISCO-RTTMON-MIB への書き込み権限あることを確認します。次は、一部のコマンド例です。

```
snmp-server view .1.3.6.1.4.1.9.9.42 ciscoMgmt included
snmp-server group v3group1 v3 priv write .1.3.6.1.4.1.9.9.42
snmp-server user user1 v3group1 v3 auth sha Cisco123 priv aes 128 Cisco123
```

（注） 詳細については、各 IOS デバイスの設定ガイドを参照し、的確なコマンドを確認してください。

Phone Status Test の作成

電話ステータステストを作成して、ネットワーク内の主要な電話機の到達可能性を監視することができます。

[Create Phone Status Test] ページを使用して電話ステータス テストを作成するには、次の手順を実行します。

始める前に

- テストを行うには、IP SLA 対応のデバイスと IP 電話（内線番号と IP アドレスを用意）が必要です。

- 電話ステータス テストでは、Cisco Prime Collaboration Assurance のデバイス インベントリからの情報は不要です。ただし、Cisco Prime Collaboration Assurance が電話に関連するデバイスを監視する場合、電話機の情報が変更されたときに電話ステータステストを更新できます。
- 電話ステータス テスト用の発信元デバイスは、Cisco Prime Collaboration Assurance で監視する必要があります。

ステップ 1 選択 **[模擬テストセンター（Synthetic Test Center）]** > **[電話ステータステスト（Phone Status Test）]**。

Cisco Prime Collaboration リリース 11.5 以降の場合

移行方法 **[模擬テスト（Synthetic Test）]** > **[電話ステータステスト（Phone Status Test）]**。

ステップ 2 [作成（Create）] をクリックします。

ステップ 3 [発信元（Source）]ペインで、デバイスセレクタを使用して発信元デバイスを選択するか、[名前（Name）] フィールドにデバイス名（または IP アドレス）を入力します。

ステップ 4 [電話レポートから追加（Add From Phone Report）] をクリックします。

ステップ 5 [エンドポイントの診断レポート（Endpoint Diagnostic report）] の[音声電話/回線レポート（Audio Phones/Lines report）]で、テストを追加する電話機の横にあるチェックボックスをオンにし、[電話の追加（Add Phones）] をクリックし ます。

ステップ 6 [Create Phone Status Test] ページの [Run] 領域で、次の手順に従います。

- テストを実行する時期をスケジュールします。
- テストの名前を入力します。
- [Cisco Prime Collaboration サーバからの ping を使用しない（Do not use ping from Cisco Prime Collaboration server）] のチェックボックスをオンにして、Cisco Prime Collaboration Assurance サーバからの ping を無効にします。

ステップ 7 **[保存（Save）]** をクリックします。

[電話ステータステスト（Phone Status Test）]ページから、電話テストの編集、表示、および削除を行うことができます。

Phone Status Test のインポート

電話ステータス テストを作成するには、テストに含める内線番号のリストを含むシード ファイルをインポートします。

始める前に

- シード ファイルの形式が正しいことを確認します。シード ファイル形式の詳細については、「Phone Status Test インポートファイルの形式」 を参照してください。

シード ファイルを使用して電話ステータス テストを作成するには、次の手順を実行します。

ステップ 1 選択 **[模擬テストセンター（Synthetic Test Center）]** > **[電話ステータステスト（Phone Status Test）]**。

Cisco Prime Collaboration リリース 11.5 以降の場合

移行方法 **[模擬テスト（Synthetic Test）]** > **[電話ステータステスト（Phone Status Test）]**。

ステップ 2 [インポート（Import）] をクリックします。[参照（Browse）] をクリックして、シード ファイルを追加します。

ステップ 3 [Run] 領域で、次の手順に従います。

- テストを実行する時期をスケジュールします。
- テストの名前を入力します。
- [Cisco Prime Collaboration サーバからの ping を使用しない（Do not use ping from Cisco Prime Collaboration server）] のチェックボックスをオンにして、Cisco Prime Collaboration Assurance サーバからの ping を無効にします。

ステップ 4 [OK] をクリックします。

Phone Status Test インポートファイルの形式

電話ステータス テストのシード ファイルは、テストするすべての電話をリストする必要があります。6 カラムまたは 8 カラムのファイル形式が使用できます。最初の 6 つのカラムは、両ファイル形式を通じて同じです。

各電話用に提供する必要がある情報は、内線番号、IP アドレス、および MAC アドレスです。手順は次のとおりです。

- 共有電話：いずれかまたは両方の電話を入力します。Cisco Prime Collaboration Assurance は、共有回線上の各電話につき、1 つのテストを実行できます。
- 複数の内線番号：電話機に複数の内線番号を入力しても、Cisco Prime Collaboration Assurance では、電話 1 台につき 1 つのテストのみを実行します。

ソフト フォンの MAC アドレス フィールドにデバイス名が表示されます。

6 カラムまたは 8 カラムのファイル形式が使用できます。最初の 6 つのカラムは、両ファイル形式を通じて同じです。シード ファイルの各行には、次のものが含まれている必要があります。

- 6 つまたは 8 つのカラム。使用しないカラムには、スペースを入力する必要があります。
- カラムはコロンで区切ります。

また、電話が登録されている Cisco Unified CM に直近のルータの IP アドレスおよびリード ライト コミュニティ ストリングを提供する必要もあります。

次の表に、電話ステータスをテストするためのシードファイル形式を示します。

表 *68 :* 電話ステータス テストのシード ファイル形式

カラム番号	説明
1	電話の内線番号。
2	電話の MAC アドレス。
3	電話の IP アドレス。
4	**Cisco Prime Collaboration リリース 11.1 以前の場合** IP SLA 対応デバイス（ルータ、スイッチ、または音声ルータ）。
5	**Cisco Prime Collaboration リリース 11.1 以前の場合** SLA 対応デバイスのリードコミュニティ ストリング。
6	**Cisco Prime Collaboration リリース 11.1 以前の場合** SLA 対応デバイスのライトコミュニティ ストリング。
7	SNMPv3 ユーザ名（8 カラム形式でだけ使用）。
8	SNMPv3 パスワード（8 カラム形式でだけ使用）。

例

Cisco Prime Collaboration リリース 11.1 以前の場合

例 1：電話のステータスをテストする 6 列のインポート ファイル

```
[拡張子]:[MACアドレス]:[IPアドレス]:[IPSLAルーター]:[コミュニティの読み取り]:[コミュニティの書き込み] 4000:200000000001:172.20.121.1:10.76.34.194:private:private
```

次の例は、8列のインポートファイルのサンプルを示しています。

例 2：電話のステータスをテストする 8 列のインポート ファイル

```
2）[拡張子]:[MACアドレス]:[IPアドレス]:[SAAルーター]:[コミュニティの読み取り]:[コミュニティの書き込み]:
[snmpv3UserName]:[snmpv3Passwd]
#4000:200000000001:172.20.121.1:10.76.34.194:!{[NOVALUE]}!:!{[NOVALUE]}!:admin:admin
```

Synthetic Test

合成テストを使用して、音声アプリケーションのアベイラビリティを確認します。これらのテストは、音声アプリケーションがユーザからのサービスリクエストを処理できるかどうかを確認します。たとえば、合成テストを使用して、電話を Cisco Unified CM に登録できるかどうかを確認できます。これらのテストは、定期的に実行するように設定できます。

合成テストでは、ユーザの操作をエミュレートすることにより、模擬電話を使用して音声アプリケーションのアベイラビリティを測定します。たとえば、合成テストでクラスタ間のコールを開始し、コールが成功したかどうかを確認します。

Cisco Prime Collaboration Assurance は、合成テストで返された情報を監視し、結果に基づきイベントを生成します。Cisco Prime Collaboration Assurance は、合成テストに合格しなかった場合には重大なイベントを生成します。そのイベントは、Event Browser に表示されます。

Cisco Prime Collaboration Assurance は、次のアプリケーションの合成テストをサポートします。

- Cisco Unified CM および Cisco Unified CM Express
- Cisco TFTP Server
- Cisco HTTP Server
- Cisco Emergency Responder
- Cisco Unity、Cisco Unity Express、および Cisco Unity Connection

（注） NAT 環境の RTP 伝送を含む合成テストの作成はサポートされません。

次の表には、合成テストと、各テストで合格するために必要な結果が示されています。

表 *69 :* 合成テストの内容と予期される結果

Synthetic Test	説明	予期される結果
Phone Registration テスト	Cisco Unified CM との接続を開いて、シミュレートされた IP フォンを登録します。	電話登録の成功。
Dial-Tone テスト	Cisco Unified CM に対するオフフック状態をシミュレートし、ダイヤル トーンが受信されるかどうかを調べます。	Cisco Unified CM からダイヤル トーン信号を受信します。

Synthetic Test	説明	予期される結果
エンドツーエンド コール テスト	2番目にシミュレートした電話または実際の IP フォンへのコールを開始します。	• 登録し、オフフック状態に移行し、コールを発信する • 着呼表示 • コールを受信する宛先電話がオフフック状態になる ユーザのエンドツーエンド コールのコール進捗音および Announcement をゲートウェイに設定すると、電話の着呼前または着呼 2 回後でもテストが成功する可能性があります。これによりユーザのゲートウェイが正しく動作していることが示されます。
TFTP ダウンロード テスト	TFTP サーバで TFTP ファイル取得操作を実行します。	TFTP サーバからの設定ファイルのダウンロードが成功します。
Cisco Prime Collaboration リリース 11.6 以降の場合 HTTP Download テスト	HTTP サーバで HTTP ファイルの取得操作を実行します。	HTTP サーバから設定ファイルを正常にダウンロードします。
緊急コール テスト	緊急番号へのコールを開始して、緊急コールのダイナミック ルーティングをテストします。	• すべてのコールが開始される • Public Safety Answering Point（PSAP）および On Site Alert Number（OSAN）の着呼表示（設定されている場合）

Synthetic Test	説明	予期される結果
Cisco Unity メッセージ待機インジケータ テスト、概要	宛先の電話にコールし、ボイスメールボックスに音声メッセージを残します。 Message-Waiting Indicator テストの宛先電話機の自動転送設定は、「呼出音を X 回鳴らした後ボイスメールに転送」と設定されている必要があります。 「コール常時転送」と設定されている場合は、テストは不合格になります。	電話のメッセージ待機インジケータをアクティブにします。その後メッセージは削除され、メッセージ待機インジケータは無効になります。

Synthetic Test の前提条件

各 Cisco Unified Communications Manager と、ネットワークでサポートされる Cisco 音声アプリケーションに対してだけ模擬テストを設定できます。各模擬テストに関係する Cisco Unified Communications Manager またはサポートされる Cisco 音声アプリケーションの中で、1 台以上の電話機を設定する必要があります。

模擬テストを作成するときは、次のガイドラインに従ってください。

- 模擬電話の MAC アドレスは、00059a3b7700 ～ 00059a3b8aff の範囲内であることと、00059a3b7700 の形式であることが必要です。
- 各テストで電話の内線番号を 1 つと MAC アドレスを 1 つ作成し、これらをテスト専用にします。
- Cisco Unified CM ごとに模擬テストを 1 つだけ設定します。
- SIP URI は、sip:extn@ccm の形式で指定してください（たとえば sip:7690@ct-sd.cisco.com）。

（注） 内線番号では次の特殊文字を使用できます：+、@、(.)、(-), ?, \,], [, (-), !, X、^、*、および #。

- テストで使用する内線番号と MAC アドレスの組み合わせは、音声クラスタを通じて一意であることを確認します。
- 模擬テストでは、Cisco 7960 IP 電話だけが模擬エンドポイントとしてシミュレートされます。
- 模擬電話機が Cisco Unified CM で事前設定されていない場合、自動登録が有効になっていると、模擬テストの初回の実行に失敗しますが、それ以降の実行は正しく動作します。

- 会議の診断と音声電話機能の模擬テストを正しく実行するには、Cisco Prime Collaboration Assurance Service Pack 1 バンドルを適用する前に、CUCM がリストされているバージョンであることを確認してください。詳細については、12.1 SP1 の『Cisco Prime Collaboration Assurance でサポートされているデバイス』を参照してください。

模擬テスト用のアプリケーションの設定や電話機の数の決定に役立つワークシートの一覧については、「Synthetic Test ワークシート」を参照してください。

Emergency Call Synthetic Test の作成

宛先電話の場合、発信 PSAP はローカル電話（911 ではない）を使用する必要があります。また、OSAN では、模擬電話だけを使用します（ローカルのオンサイトセキュリティ電話を使用しないでください）。

（注） 緊急コールの模擬テストは、Cisco Emergency Responder 1.x 以降でサポートされています。

Emergency Call 模擬テストを作成するには、次の手順を実行します。

ステップ 1 選択 **[模擬テスト（Synthetic Tests）]** > **[UCアプリケーション模擬テスト（UC Application Synthetic Test）]**。

Cisco Prime Collaboration リリース 11.5 以降の場合

移行方法 **[模擬テスト（Synthetic Tests）]** > **[UCアプリケーション模擬テスト（UC Application Synthetic Test）]**。

ステップ 2 [作成（Create）] をクリックします。

ステップ 3 [テストの種類（Test Type）] ドロップダウン メニューから、[緊急コールテスト（Emergency Call Test）] を選択します。

ステップ 4 [CER Parameters] ペインで、次の操作を実行します。

- Cisco Emergency Responder がインストールされているシステムの名前または IP アドレスを選択します。

  左ペインの Select Voice Application グループ セレクタを使用してデバイスを入力することができます。グループ セレクタでデバイスを選択してから、[Cisco Emergency Responder] フィールドの横にある矢印ボタンをクリックしてください。

- 緊急用の電話番号を入力します。

ステップ 5 [Caller] ペインで、次の操作を実行します。

- 発信者の電話に対して、Cisco Unified Communications Manager または Cisco Unified Communications Manager Express の名前または IP アドレスを選択します。

  左ペインの Select Voice Application グループ セレクタを使用してデバイスを入力することができます。Group Selector でデバイスを選択してから、[Cisco Unified Communications Manager/Express] フィールドの横にある矢印ボタンをクリックしてください。

- テスト電話機の MAC アドレスを入力します。Group Selector を使用して Cisco Unified Communications Manager または Cisco Unified Communications Manager Express システムを選択した場合は、MAC アドレス フィールドの値は自動的に入力されます。

  Cisco Prime Collaboration Assurance が唯一確認することは、[模擬テストの作成（Create Synthetic Test）] ページで入力された MAC アドレス番号の構文が有効であることです。Cisco Unified Communications Manager で設定されているとおりに、正しい番号を確実に入力してください。MAC アドレスの制限については、「Synthetic Test の前提条件」を参照してください。

ステップ 6 [PSAP] ペインで、次の操作を実行します。

- Public Safety Answering Point（PSAP）Cisco Unified Communications Manager または Cisco Unified Communications Manager Express を選択します。

  左ペインの Select Voice Application グループ セレクタを使用してデバイスを入力することができます。Group Selector でデバイスを選択してから、[Cisco Unified Communications Manager/Express] フィールドの横にある矢印ボタンをクリックしてください。

- PSAP 電話機の MAC アドレスを入力します。

ステップ 7 （オプション）オンサイトのアラート番号（OSAN）がある場合は、[オンサイトのアラート番号（On Site Alert number）] チェックボックスをオンにし、[OSAN] ペインに次の情報を入力します。

- OSAN Cisco Unified Communications Manager または Cisco Unified Communications Manager Express の名前または IP アドレス。

  左ペインの Group Selector を使用してデバイスを入力することができます。Group Selector でデバイスを選択してから、[Cisco Unified Communications Manager/Express] フィールドの横にある矢印ボタンをクリックしてください。

- OSAN 電話機の MAC アドレス。

ステップ 8 [実行（Run）] ペインで、テストの名前と実行スケジュールを設定します。

（注） [実行（Run）]ペインに入力するテスト名には、タブ、疑問符、引用符、アスタリスク、セミコロン、コンマ、コロン、スラッシュ、縦線、バックスラッシュを含めることはできません。

ステップ 9 [作成（Create）] をクリックします。

Synthetic Test メッセージ待機インジケータの作成

このテストを実行する宛先電話の要件を次に示します。

模擬テストに使用する Cisco Unity Connection で加入者を作成するときは、次の手順に従って加入者を設定します。

- [次回ログイン時に自己登録でユーザを設定（Set Subscriber for Self-Enrollment at Next Login）] チェックボックスをオフにするか、実際の電話を使用して Cisco Unity のデバイスにダイヤルし、パーソナル化プロセスを完了する必要があります。

- パスワードのオプションは、[Password never expires] に設定します。Message-Waiting Indicator テストの宛先電話機の自動転送設定は、「呼出音をX回鳴らした後ボイスメールに転送」と設定されている必要があります。「コール常時転送」と設定されている場合は、テストは不合格になります。

このテストは、SCCP エンドポイントでのみサポートされています。このテストでは、SIP エンドポイントはサポートされていません。

（注） **Cisco Prime Collaboration リリース 11.1 以前の場合**

Cisco Unified CM バージョン アップグレードを実行した後、アップグレードした Cisco Unified CM を使用する Cisco Unity の模擬テストが動作しなくなることがあります。この問題が発生した場合は、Cisco Unity 模擬テストを削除してから再び模擬テストを追加する必要があります。

模擬テストのメッセージ待機インジケータを作成するには、次の手順に従います。

ステップ 1 選択 **[模擬テスト（Synthetic Tests）]** > **[UCアプリケーション模擬テスト（UC Application Synthetic Test）]**。

Cisco Prime Collaboration リリース 11.5 以降の場合

移行方法 **[模擬テスト（Synthetic Tests）]** > **[UCアプリケーション模擬テスト（UC Application Synthetic Test）]**。

ステップ 2 [作成（Create）] をクリックします。

ステップ 3 [テストの種類（Test Type）] ドロップダウン メニューから、**[メッセージ待機インジケータテスト（Message-Waiting Indicator Test）]** を選択します。

ステップ 4 [Unity Parameters] ペインで、Cisco Unity、Cisco Unity Express、または Cisco Unity Connection システムの詳細を入力します。

ステップ 5 適切な情報を入力し、[作成（Create）] をクリックします。

TFTP Download Synthetic Test の作成

各 Cisco Unified Communications Manager に対して設定できる TFTP ダウンロード テストは 1 つのみです。

TFTP Download 模擬テストを作成するには、次の手順を実行します。

ステップ 1 選択 **[模擬テスト（Synthetic Tests）]** > **[UCアプリケーション模擬テスト（UC Application Synthetic Test）]**。

Cisco Prime Collaboration リリース 11.5 以降の場合

移行方法 **[模擬テスト（Synthetic Tests）]** > **[UCアプリケーション模擬テスト（UC Application Synthetic Test）]**。

ステップ 2 [作成（Create）] をクリックします。

ステップ 3 [テストの種類（Test Type）] ドロップダウン メニューから、[TFTPダウンロード テスト（TFTP Download Test）] を選択します。

ステップ 4 [音声アプリケーションの選択（Select Voice Application）] グループ セレクタから、設定するテストの対象である Cisco Unified CM または Cisco Unified CM Express を選択します。

ステップ 5 [実行（Run）] ペインで、テストの名前と実行スケジュールを指定します。

（注） [実行（Run）]ペインに入力するテスト名には、タブ、疑問符、引用符、アスタリスク、セミコロン、コンマ、コロン、スラッシュ、縦線、バックスラッシュを含めることはできません。

ステップ 6 [作成（Create）] をクリックします。

HTTP Download Synthetic Test の作成

Cisco Prime Collaboration リリース 11.6 以降の場合

各 Cisco Unified Communications Manager に対して設定できる HTTP ダウンロード テストは 1 つだけです。

HTTP ダウンロードの模擬テストを作成するには、次の手順を実行します。

ステップ 1 選択 **[模擬テスト（Synthetic Tests）] > [UCアプリケーション模擬テスト（UC Application Synthetic Test）]**。

ステップ 2 [作成（Create）] をクリックします。

ステップ 3 [テストタイプ（Test Type）] ドロップダウンリストで、[HTTP ダウンロードテスト（HTTP Download test）] を選択します。

ステップ 4 [音声アプリケーションの選択（Select Voice Application）] グループ セレクタから、設定するテストの対象である Cisco Unified CM または Cisco Unified CM Express を選択します。

ステップ 5 [実行（Run）] ペインで、テストの名前と実行スケジュールを指定します。

（注） [実行（Run）]ペインに入力するテスト名には、タブ、疑問符、引用符、アスタリスク、セミコロン、コンマ、コロン、スラッシュ、縦線、バックスラッシュを含めることはできません。

ファイル名を入力します。

ステップ 6 [作成（Create）] をクリックします。

End-to-End Call Synthetic Test の作成

実際の電話と模擬電話のどちらを宛先電話として設定するかを選択できます。デフォルト設定は模擬電話です。

イネーブルにされた RTP を持つ非仮想宛先電話機を含む SIP ベースのエンドツーエンド コール テストは、NAT/マルチ エンド カスタマー環境では機能しません。テストは実行されますが、シグナリングの部分のみ合格します。RTP 伝送は失敗します。

この場合、テストは Enable RTP 伝送オプションが選択された実際の電話機に対して実行されます。End-to-End Call Test は NAT 環境にある電話機にメディア伝送を行うことができません。

（注） 1 分間隔で実行されるエンドツーエンド コール テストの数が 100 個を超えないようにしてください。エンドツーエンド コール テストを追加する場合は、実行間隔を変えて、間隔を 1 分間よりも大きくしてください。

エンドツーエンド コールの模擬テストを作成するには、次の手順を実行します。

ステップ 1 選択 **[模擬テスト（Synthetic Tests）]** > **[UCアプリケーション模擬テスト（UC Application Synthetic Test）]**。

Cisco Prime Collaboration リリース 11.5 以降の場合

移行方法 **[模擬テスト（Synthetic Tests）]** > **[UCアプリケーション模擬テスト（UC Application Synthetic Test）]**。

ステップ 2 [作成（Create）] をクリックします。

ステップ 3 [テストタイプ（Test Type）] ドロップダウン メニューから、[エンドツーエンドコールテスト（End-to-End Call Test）] を選択します。

ステップ 4 [発信者（Caller）]ペインで、次の操作を実行します（選択した電話機のタイプによっては、選択が利用不可になる場合があります）。

a) Cisco Unified Communications Manager または Cisco Unified Communications Manager Express システムを入力します。

左ペインの Select Voice Application グループ セレクタを使用してデバイスを入力することができます。Group Selector でデバイスを選択してから、[Cisco Unified Communications Manager/Express] フィールドの横にある矢印ボタンをクリックしてください。

b) テスト電話機の MAC アドレスを入力します。

Group Selector を使用して Cisco Unified Communications Manager または Cisco Unified Communications Manager Express システムを選択した場合は、MAC アドレス フィールドの値は自動的に入力されます。

MAC アドレスの制限については、「Synthetic Test の前提条件」を参照してください。

c) プロトコル タイプを選択します。

d) パラメータ タイプを選択します。

- [Extension] を選択した場合は、電話機の内線番号を入力します。
- [SIP URI] を選択した場合は、SIP Uniform Resource Identifier（SIP URI）を入力します。SIP URI は、sip:extn@ccm の形式で指定してください（たとえば sip:7690@ct-sd.cisco.com）。

（注） 内線番号では次の特殊文字を使用できます：+、@、(.)、(-), ?, \,], [, (-), !, X、^、*、および #。

ステップ 5 [Recipient] ペインで、次の操作を実行します。

a) [Synthetic Phone] または [Real Phone] のオプション ボタンを選択します。

b) Cisco Unified Communications Manager または Cisco Unified Communications Manager Express システムの名前または IP アドレスを入力します（[実際の電話（Real Phone）] オプション ボタンを選択した場合、このオプションはグレー表示されます）。

左ペインの Select Voice Application グループ セレクタを使用してデバイスを入力することができます。Group Selector でデバイスを選択してから、[Cisco Unified Communications Manager/Express] フィールドの横にある矢印ボタンをクリックしてください。

c) 電話機の MAC アドレスを入力します（[実際の電話（Real Phone）]オプション ボタンを選択した場合、このオプションはグレー表示されます）。
d) プロトコル タイプを選択します（[Real Phone] オプション ボタンを選択した場合は、このオプションはグレー表示されます）。
e) パラメータ タイプを選択します（[Real Phone] オプション ボタンを選択した場合は、このオプションはグレー表示されます）。[Extension] を選択した場合は、電話機の内線番号を入力します。[SIP URI] を選択した場合は、URI を入力します。

[Synthetic Phone] を選択した場合は、[Parameters] 領域はグレー表示になっています。

ステップ 6 [Parameters] ペインで、次の操作を実行します。

- （任意）[Wait for Answer] を選択します。[Synthetic Phone] オプション ボタンを選択した場合は、このオプションはグレー表示されます。
- （任意）[Enable RTP transmission] を選択します。[Synthetic Phone] オプション ボタンを選択した場合は、このオプションはグレー表示されます。
- 合格基準として、[Call Success] または [Call Failure] を選択します。
- 必要に応じて、コールセットアップ時間しきい値の設定を変更します（デフォルトは 10000 ミリ秒）。

コールセットアップ時間しきい値は、ユーザが番号をダイヤルし終えてから Cisco Unified Communications Manager によってコールがセットアップされるまでの時間を表します（SIP または SCCP 電話機を使用）。このしきい値を超えると、警告イベントが生成されます。

ステップ 7 [実行（Run）] ペインで、テストの名前と実行スケジュールを設定します。

（注） [実行（Run）]ペインに入力するテスト名には、タブ、疑問符、引用符、アスタリスク、セミコロン、コンマ、コロン、スラッシュ、縦線、バックスラッシュを含めることはできません。

ステップ 8 [作成（Create）] をクリックします。

（注） 模擬電話機と受信者の電話機は、SCCP または SIP プロトコルのいずれかで動作できます。

Dial-Tone Synthetic Test の作成

ダイヤルトーン模擬テストを作成するには、次の手順を実行します。

ステップ 1 選択 **[模擬テスト（Synthetic Tests）] > [UC アプリケーション模擬テスト（UC Application Synthetic Test）]**。

Cisco Prime Collaboration リリース 11.5 以降の場合

移行方法 **[模擬テスト（Synthetic Tests）]** > **[UCアプリケーション模擬テスト（UC Application Synthetic Test）]**。

ステップ 2 [作成（Create）] をクリックします。

ステップ 3 [テストの種類（Test Type）] ドロップダウン メニューから、[ダイアルトーン テスト（Dial-Tone Test）] を選択します。

ステップ 4 [音声アプリケーションの選択（Select Voice Application）] グループ セレクタで、テストを設定する Cisco Unified CM または Cisco Unified CM Express システムを選択します。

ステップ 5 テスト電話機の MAC アドレスを入力します。MAC アドレスの制限については、「Synthetic Test の前提条件」を参照してください。

必要に応じて、ダイヤル トーン時間しきい値の設定を変更します（デフォルトは 500 ミリ秒）。

ダイヤルトーン時間のしきい値は、SCCP 電話がオフフック状態になった時から、Cisco Unified CM からダイヤル トーンを受信するまでの時間を示します。このしきい値を超えると、警告イベントが生成されます。

ステップ 6 [実行（Run）] ペインで、テストの名前と実行スケジュールを指定します。

（注） [実行（Run）]ペインに入力するテスト名には、タブ、疑問符、引用符、アスタリスク、セミコロン、コンマ、コロン、スラッシュ、縦線、バックスラッシュを含めることはできません。

ステップ 7 [作成（Create）] をクリックします。

（注） ダイヤルトーン模擬テストは、SCCP エンドポイントのみをサポートしています。このテストでは、SIP エンドポイントはサポートされていません。

Phone Registration Test の作成

電話機登録テストを作成するには、次の手順を実行します。

ステップ 1 選択 **[模擬テスト（Synthetic Tests）]** > **[UCアプリケーション模擬テスト（UC Application Synthetic Test）]**。

Cisco Prime Collaboration リリース 11.5 以降の場合

移行方法 **[模擬テスト（Synthetic Tests）]** > **[UCアプリケーション模擬テスト（UC Application Synthetic Test）]**。

ステップ 2 [作成（Create）] をクリックします。

ステップ 3 [テストの種類（Test Type）] ドロップダウン リストで、[電話機登録テスト（Phone Registration）] を選択します。

ステップ 4 [音声アプリケーションの選択（Select Voice Application）] グループ セレクタで、テストを設定する Cisco Unified CM または Cisco Unified CM Express を選択します。

ステップ 5 テスト電話機の MAC アドレスを入力します。MAC アドレスの制限に対する「Synthetic Test の前提条件」を参照してください。

ステップ 6 プロトコルおよびパラメータ タイプを選択します。

- [Extension] を選択した場合は、電話機の内線番号を入力します。
- [SIP URI] を選択した場合は、SIP Uniform Resource Identifier（SIP URI）を入力します。SIP URI は、sip:extn@ccm の形式で指定してください（たとえば sip:7690@ct-sd.cisco.com）。

ステップ 7 合格基準を選択します（[Registration Success] または [Registration Failure]）。

必要に応じて、登録時間しきい値の設定を変更します（デフォルトは2000ミリ秒）。電話機登録のしきい値は、電話機（SIP または SCCP電話）が Cisco Unified CM に登録されるまでの時間を表します。このしきい値を超えると、警告イベントが生成されます。

ステップ 8 [実行（Run）] ペインで、テストの名前と実行スケジュールを指定します。

（注） [実行（Run）]ペインに入力するテスト名には、タブ、疑問符、引用符、アスタリスク、セミコロン、コンマ、コロン、スラッシュ、縦線、バックスラッシュを含めることはできません。

ステップ 9 [作成（Create）] をクリックします。

Synthetic Test のインポート

複数の模擬テストを一度にインポートするには、カンマ区切り形式（CSV）ファイルを使用します。

模擬テストをインポートするには、次の手順に従います。

始める前に

- シード ファイルの形式が正しいことを確認します。詳細については、「模擬テスト インポート ファイルの形式」を参照してください。

ステップ 1 選択 **[模擬テスト（Synthetic Tests）]** > **[UCアプリケーション模擬テスト（UC Application Synthetic Test）]**。

Cisco Prime Collaboration リリース 11.5 以降の場合

移行方法 **[模擬テスト（Synthetic Tests）]** > **[UCアプリケーション模擬テスト（UC Application Synthetic Test）]**。

ステップ 2 [インポート（Import）] をクリックします。

ステップ 3 [模擬テストのインポート（Import Synthetic Test）] ページで、シード ファイルを参照し、[OK] をクリックします。

模擬テストのスケジュール時刻および日付はインポート ファイルで設定します。模擬テストをオンデマンドで実行する場合は、[今すぐ実行（Run Now）] ボタンを使用して実行できます。

模擬テスト インポート ファイルの形式

模擬テストのシード ファイルには、次の一般的な形式があります。

- インポート ファイルを手動で作成する場合は、インポート ファイルのに、プレーン テキスト コンテンツ（コンマ、AND、OR、またはパイプで区切る）を含める必要があります。
- すべての値は縦線（|）で区切る必要があります。
- スケジュールのカラムでは、次の形式を使用します。

  `MONTH,DAYSOFMONTH,DAYSOFWEEK,HOUR,MINUTE`

  - MONTH：0 ～ 11
  - DAYSOFMONTH：1 ～ 31
  - DAYSOFWEEK：0 ～ 6（0 = 日曜日）
  - DAYSOFWEEK：0 ～ 6（0 = 日曜日）
  - MINUTE：0 ～ 59

  各フィールドには、数字、範囲、カンマで区切った数字と範囲、またはアスタリスクを使用できます。

  MONTH フィールドと DAYSOFMONTH フィールドは変更できません。アスタリスク（*）を入力する必要があります。

  DAYSOFWEEK には、すべての曜日を表すアスタリスクを指定するか、曜日をカンマで区切って指定することができます。HOUR には、24 時間を表すアスタリスクか、範囲を入力できます。MINUTE には、すべての分を表すアスタリスクか、範囲を指定できます。

  DAYSOFWEEK には、すべての曜日を表すアスタリスクを指定するか、曜日をカンマで区切って指定することができます。HOUR には、24 時間を表すアスタリスクか、範囲を入力できます。MINUTE には、すべての分を表すアスタリスクか、範囲を指定できます。

  次のスケジュール タイプだけがサポートされます。

  - *;*;*;*;*：すべての日、24 時間
  - *;*;2-4;*;*：火曜日から木曜日まで、24 時間
  - *; *; *; 8-20; *：8:00 a.m. から 8:00 p.m の間のすべての日付
  - *;*;*;8;20-59:*;*;*;9-19;*:*;*;*;20;0-40：すべての日、午前 8:20 ～ 午後 8:40

Phone Registration テスト

Phone Registration テストのシード ファイルの形式

```
Registration テストの形式：
REGISTRATION|TestName|PollInterval|Schedule|CCMAddress|MACAddress|SrcPhoneProtocol|SIPURI_OR_EXTN
```

Phone Registration テストの例

```
REGISTRATION|reg test|60|*;*;*;*;*|ipif-skate.cisco.com|00059A3B7780|SCCP|4002
```

表 *70 : Phone Registration* テスト用のインポート ファイルの形式

カラム番号	説明
1	テストのタイプ：REGISTRATION。
2	テスト名
3	ポーリング間隔（Polling interval）
4	スケジュール（Schedule）
5	電話機が接続されている Cisco Unified CM
6	電話機の MAC アドレス。MAC の詳細については、Synthetic Test の前提条件を参照してください。
7	電話機のプロトコル（SCCP または SIP）
8	SIP URI または内線番号
9	顧客名

Dial-Tone テスト

Dial-tone テストのシード ファイルの形式

```
OFFHOOK|TestName|PollInterval|Schedule|CCMAddress|MACAddress
```

Dial-Tone テストの例

```
OFFHOOK|dial-tone|60|*;*;*;*;*|ipif-skate.cisco.com|00059A3B7781
```

表 *71 : Dial-Tone* テストのインポート ファイルの形式

カラム番号	説明
1	テストのタイプ：DIALTONE/OFFHOOK
2	テスト名
3	ポーリング間隔（Polling interval）
4	スケジュール（Schedule）
5	電話機が接続されている Cisco Unified CM
6	電話機の MAC アドレス。MAC の詳細については、Synthetic Test の前提条件を参照してください。
7	顧客名

End-to-End Call テスト

End-to-End Call テストのシード ファイルの形式

```
ENDTOENDTEST|TestName|PollInterval|Schedule|SrcCCM|SrcMAC|isDestRealPhone|DestCCM|DestMAC|Extn|
 WaitForAnswer|EnableRTP|SrcPhoneProtocol|SRC_SIPURI_OR_EXTN|DestPhoneProtocol
```

End-to-End Call テストの例

```
ENDTOENDTEST|endtoend test|60|*;|ipif-skate.cisco.com|00059A3B7782|FALSE
|ipif-skate.cisco.com|00059A3B7783|4002|TRUE|FALSE|S 付き|4004|Sccp
```

表 *72 : End-to-End Call* テストのインポート ファイルの形式

カラム番号	説明
1	テストのタイプ：ENDTOENDTEST。
2	テスト名
3	ポーリング間隔（Polling interval）
4	スケジュール（Schedule）
5	発信者の Cisco Unified CM
6	発信者の MAC アドレス。MAC の詳細については、Synthetic Test の前提条件を参照してください。
7	受信者の電話が実際の電話かどうか。true または false を入力します。
8	受信者の Cisco Unified CM
9	受信者の MAC アドレス。MAC の詳細については、Synthetic Test の前提条件を参照してください。
10	受信者の内線番号
11	応答待機。true または false を入力
12	RTP 伝送のイネーブル化。true または false を入力
13	電話機のプロトコル（SCCP または SIP）
14	SIP URI または内線番号
15	通知先電話機のプロトコル（SCCP または SIP）
16	顧客名

TFTP Download テスト

TFTP Download テストのシード ファイルの形式

```
TFTP テストの形式：TFTP|TestName|PollInterval|Schedule|CCMAddress
```

TFTP Download テストの例

```
TFTP|tftp download|60|*;*;*;*;*|ipif-skate.cisco.com
```

表 *73 : TFTP Download* テストのインポート ファイルの形式

カラム番号	説明
1	テストのタイプ：TFTP
2	テスト名
3	ポーリング間隔（Polling interval）
4	スケジュール（Schedule）
5	Cisco Unified CM
6	顧客名

Cisco Prime Collaboration リリース 11.6 以降の場合

HTTP Download テスト

HTTP Download テストのシード ファイルの形式

```
HTTP test format: HTTP|TestName|PollInterval|Schedule|CCMAddress|PhoneConfigurationFileName
```

HTTP Download テストの例

```
HTTP|HTTP Download Test|60|*;*;*;*;*|10.78.86.158|SEPDefault.cnf
```

表 *74 : HTTP Download* テストのインポート ファイルの形式

カラム番号	説明
1	テストのタイプ：HTTP
2	テスト名
3	ポーリング間隔（Polling interval）
4	スケジュール（Schedule）
5	Cisco Unified CM
6	電話機の設定ファイルの名前

Message Waiting Indicator テスト

Message-Waiting Indicator テストのシード ファイルの形式

```
End-to-End Call テストの形式：
MWITEST|TestName|PollInterval|Schedule|UnityAddress|SrcCCM|SrcMAC|DestCCM|DestMAC|Extn|Password
```

Message-Waiting Indicator テストの例

```
MWITEST|mwi test|300|*;*;*;*;*|10.76.91.155|10.76.91.148|00059A3B7B00|10.76.91.148
|00059A3B7B01|71418001|13579
```

表 *75 : Message-Waiting Indicator* テストのインポート ファイルの形式

カラム番号	説明
1	テストのタイプ：MWITEST
2	テスト名
3	ポーリング間隔（Polling interval）
4	スケジュール（Schedule）
5	Cisco Unity システム
6	発信者の Cisco Unified CM
7	発信者の MAC アドレス。MAC の詳細については、Synthetic Test の前提条件を参照してください。
8	受信者の Cisco Unified CM
9	受信者の MAC アドレス。MAC の詳細については、Synthetic Test の前提条件を参照してください。
10	受信者の内線番号
11	受信者のボイスメール パスワード
12	顧客名

Emergency Call テスト

Emergency Call テストのシード ファイルの形式

```
Emergency Call テストの形式：
EMERGENCYCALLTEST|TestName|PollInterval|Schedule|CERAddress|SrcCCM|SrcMAC|PsapCCM|PsapMAC|EmergencyNumber|enableOsan|OsanCCM|OsanMAC
```

Emergency Call テストの例

```
Emergency Call テストの形式：
EMERGENCYCALLTEST|600|*;*;*;*;*|10.76.35.211|10.76.93.75|00059A3B7789
|10.76.93.75|00059A3B7790|911|TRUE|10.76.38.111|00059A3B7791
```

表 *76 : Emergency Call* テスト

カラム番号	説明
1	テストのタイプ：CCCTEST

カラム番号	説明
2	テスト名
3	ポーリング間隔（Polling interval）
4	スケジュール（Schedule）
5	Cisco Emergency Responder システム
6	発信者の Cisco Unified CM
7	発信者の MAC アドレス。MAC の詳細については、Synthetic Test の前提条件を参照してください。
8	公安応答局（PSAP）Cisco Unified Communications Manager
9	PSAP の MAC アドレス。MAC の詳細については、Synthetic Test の前提条件を参照してください。
10	Emergency number
11	On Site Alert Number（OSAN）のイネーブル化。true または false を入力します。
12	OSAN Cisco Unified CM
13	OSAN の MAC アドレス
14	顧客名

Synthetic Test の管理

[模擬テスト（Synthetic Tests）] ページから実行できるタスクを次の表に示します。

タスク	説明
合成テストのエクスポート	作成した模擬テストを Cisco Prime Collaboration Assurance サーバ上のファイルにエクスポートできます。必要に応じて、このファイルを使用して、設定した模擬テストを Cisco Prime Collaboration Assurance にインポートしたり、テストを別の Cisco Prime Collaboration Assurance システムにインポートしたりすることができます。
模擬テストの編集	電話の内線番号および MAC アドレスが必要なテストを作成および編集する場合は、これらを常にペアで編集する必要があります。いずれかを単独で編集しないでください。 模擬テストの編集中に、MAC アドレスがすでに使用されていることを示すエラー メッセージが表示された場合は、模擬テストを削除し、同じ MAC アドレスを使用してテストを再度追加します。

タスク	説明
模擬テストの詳細の表示	[Synthetic Test Details] ページでは、テストに対して設定されているパラメータを見ることができます。 表示される詳細情報は、テストのタイプによって異なります。
模擬テストの開始と停止	模擬テストを開始または停止できます。複数の模擬テストを一度に選択して開始または停止できます。テストの実行中にテストを停止をしようとすると、テストの詳細を示すメッセージが表示されます。
模擬テスト結果の表示	結果はレポート形式で表示されます。Cisco Prime Collaboration Assurance の各種レポートと同様に、レポートを印刷したり、ファイルにエクスポートしたりすることができます。 [Synthetic Tests Results] レポートに表示される情報は次のとおりです。 • テストのステータス（合格または不合格）。 • テスト終了の日時。 • エラー メッセージ（ある場合）。
模擬テストのスケジュール	模擬テストを作成するときに、テストをすぐに実行するか、一定の時間間隔で実行するようにスケジュールするかを選択できます。 テストを実行する時刻を変更するには、[Edit Synthetic Test] ページで模擬テストを編集する必要があります。 Cisco Prime Collaboration Assurance サーバのシステム時間を過去の時刻に変更した場合、時間が経過し、システム時刻を変更する前に最初に設定した時刻に達するまで、模擬テストは実行されません。 たとえば、午前 10:00 にシステム時刻が午前 9:00 に変更された場合は、システム時刻が午前 10:00 にならなければテストは開始されません。 ユーザがこのタスクを実行できるかどうかは、ユーザのログインによって決まります。

模擬テストに関する特記事項

次の表に、模擬テストの作成中に注意すべき情報を示します。

概要	説明
模擬テストは、Cisco Prime Collaboration Assurance の処理開始後 30 分間は実行されません。ただし、この間にテストを作成、編集または削除することはできます。	Cisco Prime Collaboration Assurance プロセスを開始すると、システムに高い負荷がかかります。合成テストの失敗を防ぐには、Cisco Prime Collaboration Assurance の開始を遅らせます。

概要	説明
模擬テストは、サーバ CPU RAM が 85 % に達するとスキップされるか、または実行するには長時間を要する場合があります。 この異常はポートレットに反映されます。	サーバの CPU が 85 % を超えていれば、模擬テストはスキップされるか実行により長い時間がかかります。 したがって、これらのテストに関するポートレットのデータは、1 時間あたりにスケジュールされるよりも少ない回数のテストを表します。この状況を回避するには、オフピーク時にテストをスケジュールします。
模擬テストの間隔の値を小さくすると、新しい値で最初の結果がレポートされるのに新しい時間間隔以上に長くかかる場合があります。	それぞれの模擬テストは、時間間隔設定で制御された時刻に実行されます。模擬テストの時間間隔の設定を小さくした直後は、新しい間隔よりも経過時間が長くなるまで、トランザクションが実行されないことがあります。 たとえば、時間間隔を 180 秒から 60 秒に減らした場合、新しい間隔で実行された最初の結果は、レポートされるまでに 240 秒もの長さを必要とする場合があります。
1 回限りの模擬テストは失敗することがあります。	1 回だけ実行される模擬テストは、たまに失敗する場合があります。このような失敗は、Cisco Prime Collaboration Assurance の負荷が大きいことや、Cisco Prime Collaboration Assurance がアプリケーションから受信できないイベントがあることが原因となっている可能性があります。
Cisco Unity Message-Waiting Indicator 模擬テストは失敗することがあります。	Cisco Unity Connection 模擬テストが失敗したときに、Message-Waiting Indicator ライトがオンになっている場合は、テストで使用したのと同じ内線番号で実際の電話を設定し、ボイスメールを手動で削除する必要があります。 あるいは、Message Store Manager ツールを使用してボイスメールを削除することもできます。これを完了すると、テストにパスします。
NAT 環境で、End-to-end Call テストが失敗する可能性があります。	電話機が NAT 環境にある場合、End-to-End Call 模擬テストはサポートされません。この場合、テストは Enable RTP 伝送オプションが選択された実際の電話機を対象とします。End-to-End Call 模擬テストは、NAT 環境にある電話機にメディア伝送を行うことができません。

IP SLA 音声テスト

IP SLA Voice テストは、エンド ツー エンドとホップ バイ ホップの両方で、マルチプロトコル ネットワークの応答時間と可用性を監視します。このデータを収集した後、Cisco Prime Collaboration Assurance のグラフ機能を使用して、ネットワーク パフォーマンス メトリックの変更を確認できます。ネットワーク パフォーマンス データをリアルタイムに選択、表示、図化することができます。ネットワーク デバイスの IP SLA を理解して導入するには、Cisco.com の「IP サービスレベル契約（IP SLA）」テクノロジ ページを参照してください。

前提条件：

- Cisco IOS IP SLA のソースとレスポンダをネットワークに設定する必要があります。
- Cisco Prime Collaboration Assurance インベントリを使用して、がデバイスで IPSLA レスポンダ機能が有効になっているかどうか確認します。
- IP SLA 音声テストを設定するときは、SNMP クレデンシャルでコミュニティ ストリングの読み取り/書き込みが有効になっていることを確認します。

IP SLA Voice テストは、特定のしきい値を超えたときにイベントがトリガーされるように設定できます。

IP SLA Voice テストは 1 つずつ作成するか、ファイルをインポートして複数のテストを同時に作成できます。

次のIP SLA Voice テストを作成できます。

テスト名	説明
UDP Jitter for VoIP	Cisco Prime Collaboration Assurance プロセスを開始すると、システムに高い負荷がかかります。合成テストの失敗を防ぐには、Cisco Prime Collaboration Assurance の開始を遅らせます。 模擬的な UDP トラフィックを生成することにより、パケット損失、ラウンドトリップ遅延、および IP ネットワークの遅延の変動（ジッター）を測定します。 このテストでは、UDPプロトコルを使用して、遅延、一方向のジッタ、およびパケットのドロップを測定します。ジッタとは、パケット間の遅延です。発信元デバイスは、指定されたパケット間遅延で宛先デバイスに一定数のパケットを送信します。 宛先（IP SLA Responder）は、パケットにタイムスタンプを記録し、パケットを返送します。このデータを使用して、一方向のプラスおよびマイナスのジッタ（発信元から宛先およびその逆方向）、パケット損失（発信元から宛先およびその逆方向）、およびラウンドトリップ遅延を調べます。 プラスのジッタは、パケットの一方向の遅延が直前のパケット遅延より長い場合に発生します。マイナスのジッタは、パケットの一方向の遅延が直前のパケット遅延より短い場合に発生します。この連続した数値がばらばらに乱れている場合、テストはエラーを示しています。
Ping Echo	発信元デバイスと任意の IP 対応デバイス間のエンドツーエンドの応答時間を測定します。 テストでは、発信元デバイスから宛先デバイスに ICMP パケットを送信し、ラウンドトリップの完了にかかる時間を測定します。
Ping Path Echo	traceroute を使用してパスを検出し、発信元デバイスとパスに含まれる各ホップ間の応答時間を測定することにより、発信元デバイスとネットワーク上の任意の IP デバイス間のホップバイホップの応答時間を測定します。 （注） Round-Trip Response Time しきい値を変更する場合は、[Thresholds] ペインのチェックボックスをオンにして、新しい設定を入力します（デフォルトは 300 m/sec）。この設定は正の整数（32 ビット）にする必要があります。

テスト名	説明
UDP Echo	発信元デバイスと任意の IP 対応デバイス間の UDP 応答時間を測定します。 UDP Echo テストでは、設定された数のバイトからなるパケットを指定されたポート番号の宛先に送信し、応答時間を測定します。 UDP Echo 操作には、IP SLA を使用する RTR Responder と IP SLA を使用しない UDP サーバの 2 つの宛先デバイス タイプがあります。
Gatekeeper Registration Delay	ゲートウェイをゲートキーパーに登録するために必要な時間を測定します。 このテストでは、H.323 ゲートウェイから H.323 ゲートキーパーに軽量の登録要求（RRQ）を送信し、ゲートキーパーから登録確認（RCF）を受信します。その後、この応答時間が測定されます。 Gatekeeper Registration Delay テストを実行する場合は、発信元ゲートウェイに SIP または H323 が設定されている必要があります。

テスト名	説明
リアルタイム転送プロトコル	DSP ソフトウェアと統合することによって、DSP から DSP への音声品質メトリックを測定します。この操作には、発信元ゲートウェイから宛先へのコール テストの実行、実際の RTP パケットの送信、DSP からの統計情報の収集が含まれます。 このテストでは、DSP ソフトウェアと統合することによって、音声品質メトリックの DSP 間の測定を実行します。テスト コールは 送信元ゲートウェイから宛先ゲートウェイに送信され、実際のリアルタイム プロトコル（RTP）パケットを送信し、DSP から統計情報を収集します。 一部のネットワークでは、リモート エンドに DSP がない場合があります。このような場合、リアルタイム プロトコル テストではリモート エンド ループを RTP ストリームに戻すことによって、メトリックを測定する必要があります。 リアルタイム転送プロトコルテストには、これらの測定における音声パス（発信元のゲートウェイでのテレフォニー インターフェイスから IP インターフェイスへのパスと、終端ゲートウェイでの IP インターフェイスからテレフォニー インターフェイスへのパス）での遅延が含まれます。 （注） リアルタイム トランスポート プロトコル テストを実行するには、送信元に C5510 または C549 のいずれかの DSP モジュール タイプが含まれており、音声ポートで ds0-group を設定する必要があります。

IP SLA Voice テストで得られたデータ結果の保存期間は 30 日です。IP SLA Voice テストまたはパフォーマンスのポーリング データ ファイルを保存期間よりも長く保存する場合、バックアップするか、フォルダまたはサーバに移動させます。

（注） isco Prime Collaboration Assurance をアンインストールする前には、必ずアプリケーションからすべてのIP SLA 音声テストを削除します。これらのテストを削除しないと、ルータでテストの実行が続行されます。

SNMP V3 クレデンシャルを使用して IP SLA 対応デバイスを管理した場合は、CISCO-RTTMON-MIB への書き込み権限あることを確認します。次は、一部のコマンド例です。

```
snmp-server view .1.3.6.1.4.1.9.9.42 ciscoMgmt included
snmp-server group v3group1 v3 priv write .1.3.6.1.4.1.9.9.42
snmp-server user user1 v3group1 v3 auth sha Cisco123 priv aes 128 Cisco123
```

（注） 詳細については、各 IOS デバイスの設定ガイドを参照し、的確なコマンドを確認してください。

Cisco IOS および IP SLA の必要なバージョン

IP SLA Voice テストは、Cisco IOS IP SLA テクノロジに依存しています。次の表には、IP SLA Voice テストを正常に設定して実行するために必要な IP SLA および Cisco IOS のバージョンが示されています。

テスト	IP SLA	Cisco IOS
Ping Echo	2.1.0 以降	12.0(5)T、12.1(1)、およびそれ以降
Ping Path Echo		
UDP Echo		
UDP Jitter for VoIP ICPIF/MOS 値を使用しません。		
UDP Jitter for VoIP ICPIF/MOS 値を使用します。	2.2.0 以降	12.3(4)T 以降
Gatekeeper Registration Delay		12.3(14)T 以降
リアルタイム転送プロトコル	2.20 以降	• タイプ - ds0-group の音声ポート。 • タイプ C5510 または C549 の DSP。 • 12.4(19.12)T 以上の IOS バージョン

[IP SLA音声テスト（IP SLA Voice Test）] を作成します。

[IP SLA音声テスト（IP SLA Voice Test）]を作成するには、次の手順を実行します。

ステップ 1 選択 **[模擬テストセンター（Synthetic Test Center）]** > **[IP SLA音声テスト（IP SLA Voice Test）]**。

Cisco Prime Collaboration リリース 11.5 以降の場合

移行方法 **[模擬テスト（Synthetic Tests）]** > **[IP SLA音声テスト（IP SLA Voice Test）]**。

ステップ 2 [作成（Create）] をクリックします。

ステップ 3 [Test Type] ドロップダウン メニューから、次のいずれかを選択します。

- VoIP 用 UDP ジッター。パラメータの詳細については、「VoIP 用 UDP ジッター テスト パラメータ」表 77 : VoIP 用 UDP ジッタ テスト パラメータ （617 ページ）を参照してください。
- Ping Echo。パラメータの詳細については、「Ping Echo テスト パラメータ」表 79 : Ping Echo テストのパラメータ （618 ページ）を参照してください。
- Ping Path Echo。パラメータの詳細については、「表 80 : Ping Path Echo テストのパラメータ」を参照してください。
- UDP Echo。パラメータの詳細については、「表 81 : UDP Echo テストのパラメータ 」を参照してください。
- Gatekeeper Registration Delay
- Real-time Transport Protocol（リアルタイム転送プロトコル）。パラメータの詳細については、「表 82 : リアルタイム転送プロトコル テスト パラメータ 」を参照してください。

ステップ 4 [Source] ペインで、次の手順に従います。

- デバイス セレクタを使用して発信元デバイスを選択します。

  最近追加した IP SLA 対応デバイスが、[IP SLA音声テストの設定（IP SLA Voice Test Configuration）] ダイアログボックスの [発信元（Source）] ペインのセレクタ内の IP SLA デバイス グループに表示されない場合は、デバイス グループ メンバーシップを更新します（**[デバイスインベントリ（Device Inventory）]** > **[インベントリ管理（Inventory Management）]**。

  Cisco Prime Collaboration リリース 11.5 以降の場合

  最近追加した IP SLA 対応デバイスが、[IP SLA音声テストの設定（IP SLA Voice Test Configuration）] ダイアログボックスの [発信元（Source）] ペインのセレクタ内の IP SLA デバイス グループに表示されない場合は、デバイス グループ メンバーシップを更新します（**[インベントリ（Inventory）]** > **[インベントリ管理（Inventory Management）]**。

- 発信元インターフェイス設定を選択します。[デフォルト（Default）] のままにするか、新しい設定を入力します。

ステップ 5 [Destination] ペインで、デバイス セレクタを使用して宛先デバイスを選択します。

発信元デバイスと宛先デバイスを切り替える場合は、[Swap Source and Destination] ボタンをクリックします。

ステップ 6 [Parameters] ペインで必要な情報を入力します。

ステップ 7 [Threshold] ペインで、必要な情報を入力します。

ステップ 8 [実行（Run）] ペインで、テストの名前と実行スケジュールを指定します。

（注） [実行（Run）]ペインに入力するテスト名には、タブ、疑問符、引用符、アスタリスク、セミコロン、コンマ、コロン、スラッシュ、縦線、バックスラッシュを含めることはできません。

ステップ 9 **[保存（Save）]** をクリックします。

例

表 *77 : VoIP* 用 *UDP* ジッタ テスト パラメータ

パラメータ	デフォルト値	使用可能な値	説明
Codec Type	—	• G.711ulaw • G.711alaw • G.729	パケット間隔および要求ペイロードの決定に使用されます。
Call Duration	8	1 ～ 59 秒	コールの時間。
Voice Quality Expectation	Land line	• Land line • Wireless campus • Wireless on the move • Multi-hop	Mean Opinion Score（MOS）および Calculated Planning Impairment Factor（ICPIF）の Access Advantage ファクタに対応します。
IP QoS	IP Precedence	• IP Precedence • DSCP	IP SLA パケットの Quality of Service ポリシーを定義します。
	5	• IP Precedence：0（なし）～ 7（高） • DSCP：0（なし）～ 8（CS1）、9、10（AF11）	これは、タイプ オブ サービス（TOS）に変換されてデバイスに設定されます。

表 *78 : VoIP* 用 *UDP* ジッタ しきい値設定

パラメータ	デフォルト値	使用可能な値	説明
Source to Destination	3（パケット損失） 40 ミリ秒（ジッター）	正の整数すべて [1]	パケット損失およびジッタのしきい値設定
Destination to Source	3（パケット損失） 40 ミリ秒（ジッター）		パケット損失およびジッタのしきい値設定
Average Latency	300 ミリ秒		遅延のしきい値設定

パラメータ	デフォルト値	使用可能な値	説明
Node-to-Node Quality	可	Excellent、Good、Fair、または Poor	テストの品質のしきい値設定です。これらの値は MOS スコアに関連付けられます。値と同等の MOS は次のとおりです。 • Excellent：5（500） • Good：4（400-499） • Fair：3（300-399） • Poor：2（200-299） • Bad：1（100-199）

表 *79 : Ping Echo* テストのパラメータ

パラメータ	デフォルト値	使用可能な値	説明
Request Payload	32 バイト	28 ～ 16384 バイト	デフォルト ICMP PING パケットは 32 バイトです。サイズを変えて操作可能です。
IP QoS	IP Precedence	• IP Precedence • DSCP	IP SLA パケットの Quality of Service ポリシーを定義します。
	0（なし）	• IP Precedence：0（なし）～ 7（高） • DSCP：0（なし）～ 8（CS1）、9、10（AF11）	これは TOS に変換されてデバイスに設定されます。

表 *80 : Ping Path Echo* テストのパラメータ

パラメータ	デフォルト値	使用可能な値	説明
Request Payload	32 バイト	28 ～ 16384 バイト	デフォルト ICMP PING パケットは 32 バイトです。サイズを変えて操作可能です。
IP QoS	IP Precedence	• IP Precedence • DSCP	IP SLA パケットの Quality of Service ポリシーを定義します。
	0（なし）	• IP Precedence：0（なし）～ 7（高） • DSCP：0（なし）～ 8（CS1）、9、10（AF11）	これは TOS に変換されてデバイスに設定されます。

表 *81 : UDP Echo* テストのパラメータ

パラメータ	デフォルト値	使用可能な値	説明
Request Payload	16 バイト	4 ～ 1500 バイト	サイズを変えて操作可能です。
IP QoS	IP Precedence	• IP Precedence • DSCP	IP SLA パケットの Quality of Service ポリシーを定義します。
	0（なし）	• IP Precedence：0（なし）～ 7（高） • DSCP：0（なし）～ 8（CS1）、9、10（AF11）	これは TOS に変換されてデバイスに設定されます。

表 *82 :* リアルタイム転送プロトコル テスト パラメータ

フィールド	説明
一般的なパラメータ テストの一般情報。	

フィールド	説明
Codec Type	パケット間隔および要求ペイロードの決定に使用されます。
Call Duration	テストの期間。デフォルトは 20 秒です。
Voice Quality Expectation	Mean Opinion Score（MOS）および Calculated Planning Impairment Factor（CPIF）の Access Advantage ファクタに対応します。
しきい値パラメータ リアルタイム転送プロトコル テストのしきい値設定。	
Interarrival Jitter	しきい値設定宛先から発信元方向での Inter-Arrival ジッタ（ミリ秒）メトリクスがサポートされます。
パケット損失	しきい値設定宛先から発信元方向での Packet Loss（数値）メトリクスがサポートされます。
R Factor	しきい値設定遅延、ジッター、パケット損失など、ITU-T 勧告 G.107 によって他の VoIP メトリックから算出される数値スコア。標準範囲は 50 ～ 90 で、80 以上のスコアは、VoIP コール品質が十分であることを示しています。デフォルトは40です。
Conversational Quality	しきい値設定設定（Excellent、Good、Fair、および Poor）に基づいて、通話のオーディオ信号を追跡します。デフォルトは Fair です。
Listening Quality	しきい値設定設定（Excellent、Good、Fair、および Poor）に基づいて、聴取のオーディオ信号を追跡します。デフォルトは Fair です。
操作固有パラメータ テスト実行のタイミングと頻度。	
Polling Time	24 時間の間にポーリングが発生する回数（分）。
Occurrence Pattern	テストが開始および終了される日付、およびその期間にテストの実行がスケジュールされた時間。テストを毎週実行する場合、スケジュールパラメータにはテストの実行がスケジュールされた曜日が表示されます。
テスト名	ユーザ定義の名前。また、Cisco Prime Collaboration Assurance では、テストデータが保存されているフォルダーの名前がテストの名前となります。この表の Data Directory フィールドの説明を参照してください。

[複数をインポート（Import Multiple）][IP SLA音声テスト（IP SLA Voice Tests）]

シード ファイルをインポートすることによって、Cisco Prime Collaboration Assurance でサポートしているテストを最大 64 つまでインポートすることができます。

複数のテストをインポートするには、次の手順を実行します。

始める前に

- テストをインポートする前に、発信元デバイスを追加する必要があります。
- シード ファイルが正しい形式であることを確認します。
- NAT 対応デバイスの IP SLA 音声テスト を構成するには、インポート ファイルに、パブリック/グローバル IP アドレスではなく、ターゲット ルータのプライベート IP アドレスまたはローカル IP アドレスが含まれていることを確認します。

ステップ 1 選択 **[模擬テストセンター（Synthetic Test Center）]** > **[IP SLA音声テスト（IP SLA Voice Test）]**。

Cisco Prime Collaboration リリース 11.5 以降の場合

移行方法 **[模擬テスト（Synthetic Tests）]** > **[IP SLA音声テスト（IP SLA Voice Test）]**。

ステップ 2 [インポート（Import）] をクリックします。

ステップ 3 [OK] をクリックします。

Cisco Prime Collaboration Assurance では、次の操作が実行されます。

- これが前にインポートしたファイルである場合、Cisco Prime Collaboration Assurance では、Cisco Prime Collaboration Assurance にデバイスが存在するかどうかが確認されます。インポート ファイル内のすべての情報が、Cisco Prime Collaboration Assurance にすでに存在する情報と同じである場合、その旨のメッセージが表示されます。**[OK]**をクリックします。
- インポート ファイルの形式に問題がある場合は、Cisco Prime Collaboration Assurance ではエラーメッセージが表示されます。[OK] をクリックしてファイルを開き、表示されている問題を修正してください。すべての問題を修正するまでファイルをインポートできません。
- エラーがない場合は、確認のダイアログボックスが表示されます。ダイアログボックスには、作成された新しいテストの数と、アップデートされるテストの数が表示されます。**[はい（Yes）]** をクリックします。

（IP SLA 音声テスト）のインポート ファイルの形式

最大で 64 テストをインポートできます。これは、Cisco Prime Collaboration Assurance が一度にサポートできる最大数です。

すべてのテスト シード ファイルには、次の情報が必要です。

- テスト名

- 操作タイプ
- 発信元デバイス名
- 宛先デバイスの情報（NAT-enabled デバイスの場合、デバイスのプライベート IP アドレスが必要です）
- 操作パラメータ
- スケジュール パラメータ

テスト シード ファイルの一般的な形式は、次のとおりです。

- インポート ファイルを手動で作成する場合は、インポート ファイルのに、プレーン テキスト コンテンツ（コンマ、AND、OR、またはパイプで区切る）を含める必要があります。
- すべての値をカンマで区切る必要があります。
- 開始日と終了日は、mm/dd/yyyy の形式になっている必要があります。たとえば、12/01/2004 です。
- 開始時刻と終了時刻は、24 時間表記の hh:mm 形式である必要があります。たとえば、23:30 です。
- 発信元 IP アドレスの入力はオプションです。このアドレスは、代替テスト アドレスと同じです。
- オプション フィールドに入力するときには、"" のように、二重引用符を付けます。
- 1 週間のすべての曜日を指定する場合は、1 を入力します。これ以外の場合は 0 を指定する必要があります。1 週間のすべての曜日のエントリが 0 の場合は、該当する曜日を入力する必要があります。曜日は縦棒（|）で区切ります。たとえば、Mon|Tue|Thu|Fri のようになります。

Ping Echo テストのインポート ファイル

インポート ファイルの形式

```
<testName>,Ping-Echo,<source>,<source-ip-address>,<Destination-Name>,<sample-interval>,

<IPQosType><IPQosValue>,<request-payload>,<LSRHop1|LSRop2|LSRHop3|LSRHop4|LSRHop5|LSRHop6|LSRHop7|LSRHop8>,
 <completionTimeThreshold or "">,<start-time>,<end-time>,<AllDaysOfWeek. 1 for all days
 otherwise 0>,<DaysOfWeek, if AllDaysOfWeek is 0>
```

LSRHop<number> はオプションのフィールドです。

インポート ファイルの例

```
echo-import1,Ping-Echo,source-1,",",dest-1,1,DSCP,9,64,lsr-hop1|lsr-hop2,300,09:00,17:00,1

echo-import2,Ping-Echo,source-1,",,dest-1,1,IPPrecedence,4,64,lsr-hop1|lsr-hop2,",
09:00,17:00,0,月||wed|
```

Ping Path Echo テストのインポート ファイル

インポート ファイルの例

```
ping-path-import2,Ping-Path-Echo,source-2,"",dest-2,3,DSCP,10,32,250,17:00,23:00,0,
mon|tue|wed|thu|fri

ping-path-import2,Ping-Path-Echo,source-2,"",dest-2,3,IPPrecedence,5,32,"",17:00,23:00,1
```

UDP Echo テスト

インポート ファイルの形式

```
udp-import2,UDP-Echo,source-1,",udp-dest,IPSLA-Responder,1,DSCP,48,2001,32,",17:00,23:00,1
```

宛先タイプは、UDP-Server または IPSLA-Responder です。

VoIP テストのための UDP ジッタ

コーデックを使用しないインポート ファイル形式（IP SLA 音声品質）のサポート

インポート ファイルの例

宛先タイプは、UDP-Server または IPSLA-Responder です。

コーデックを使用するインポート ファイル形式（IP SLA 音声品質）のサポート（Cisco IOS バージョン 12.3(4)T 以降に対して有効）

```
<testName>,Data-Jitter,<source>,<source-ip-address>,<IPSLA-Responder>,<sample-interval>,

<IPQosType>,<IPQosValue>,<codecType>,<voiceQualityBenchMark>,<number-of-packets>,<destination-port>,
 <pktlossSDThreshold or "">,<pktlossDSThreshold or "">,<jitterSDThreshold or
"">,<jitterDSThreshold or "">, <avgLatencyThreshold or "">,<nodeToNodeQualityThreshold
or "">,<start-time>,<end-time>,<AllDaysOfWeek. 1 for all days otherwise 0>,<DaysOfWeek,if
 AllDaysOfWeek is 0>
```

インポート ファイルの例

```
ジッター-import2,データ ジッター,送信元-1,送信元
-1,dest-with-IPSLA-Responder,3,IPPrecedence,5,G.711ulaw,陸上
線,20,2002,30,30,25,25,50,",17:00,23:00,1
```

リード（Read）コミュニティ ストリングはオプションのフィールドです。コミュニティ文字列を指定すると、Cisco Prime Collaboration Assurance が IP SLA のレスポンダを検証します。

VoIP Gatekeeper Registration Delay テスト（毎日のスケジュール）

コーデックを使用しないインポート ファイル形式（IP SLA 音声品質）のサポート

```
<testName>,Voip-GKReg-Delay,<source GateWay>,<sample-interval>,
<GatekeeperRegistrationTimeThresholdor "">,<start-time>,<end-time>,<AllDaysOfWeek. 1 for
 all days otherwise 0>, <DaysOfWeek, if AllDaysOfWeek is 0>
```

インポート ファイルの例

```
gkregdelay-import1,Voip-GKReg-Delay,source-gateway,3,50,17:00,23:00,0,mon|tue|wed|thu|fri
 gkregdelay-import2,Voip-GKReg-Delay, source-gateway,5,"",17:00,23:00,1
```

宛先タイプは、UDP-Server または IPSLA-Responder です。

[IP SLA音声テスト（IP SLA Voice Tests）] の管理

次の表では、[IP SLA音声テスト（IP SLA Voice Test）] ページから実行できるタスクを示します。

タスク	説明
[IP SLA音声テスト（IP SLA Voice Tests）] の編集	この機能を使用して、既存のテストのパラメータを編集することができます。たとえば、テストの操作パラメータを変更したり、スケジュールを変更することができます。宛先デバイスを変更できません。テストを編集するには、編集するテストを選択し、[編集（Edit）] をクリックします。
[IP SLA音声テスト（IP SLA Voice Tests）] の削除	この機能を使用して、1 つ以上のテストを削除することができます。どのような状態のテストでも削除できます。テストを削除するには、編集するテストを選択し、[削除（Delete）] をクリックし ます。
テスト トレンドの表示	ネットワーク パフォーマンス メトリックでは変更を選択して確認できます。ネットワーク パフォーマンスデータをリアルタイムに選択、表示、図化することができます。テストのトレンドを表示するには、トレンドを表示するテストを選択し、[トレンド（Trend）] をクリックし ます。 VOIP テスト用の UDP ジッターを選択した場合は、グラフを選択するオプションが表示され、[IP SLA 音声テスト（IP SLA Voice Test）] の傾向グラフが表示されます。その他の[IP SLA音声テスト（IP SLA Voice Test）] では、[グラフの選択（graph selection）] オプションは表示されません。
テスト情報の表示	[Test Details] ページでは、特定のテストに関するすべての詳細情報を確認できます。このページから、テスト情報を印刷またはエクスポートすることができます。テスト情報を表示するには、表示するテストを選択し、[表示（View] をクリックします。

タスク	説明
テストの詳細をエクスポートする	[Test Details] ページに表示された単一のテストの詳細情報を、設定やステータスも含めてすべてエクスポートし、保存することができます。 Internet Explorer ブラウザからテストの詳細をエクスポートする場合、[Windowsセキュリティ（Windows Security ）] ポップアップ ウィンドウでは、クレデンシャルの入力プロンプトメッセージが表示されることがあります。[Windows セキュリティ（Windows Security）] ポップアップをキャンセルして、[保存（Save）] または [名前を付けて保存（Save as）] をクリックすると、レポートをダウンロードできます。 テストの詳細をエクスポートするには、以下を実行します。 1. 必要なテストを選択し、[表示（View）] をクリックします。 2. ウィンドウの右上隅にある [エクスポート（Export）] アイコンをクリックします。

IP SLA 音声テストの結果

テストの作成中または変更中に設定したしきい値設定によって、[IP SLA音声（IP SLA Voice）] イベントが生成されるタイミングが決まります。

イベントは、発信元デバイスで発生します。3回のポーリング サイクルで連続してしきい値違反が発生すると、しきい値イベントが生成されます。このイベントは、次のポーリング サイクルで値がしきい値より小さくなるとクリアされます。[IP SLA音声（IP SLA Voice）] イベントは、次の手順で生成できます。

表 *83 : [IP SLA*音声テスト（*IP SLA Voice Test*）*]* イベント

NodeToNodeTestFailed IP SLA 音声テストが失敗した原因と解決策を確認するには、Cisco.com の IP SLA ドキュメントを参照してください。	PacketLossSD_ThresholdExceeded	RFactorDS_ThresholdExceeded
RoundTripResponseTime _ThresholdExceeded	PacketLossDS_ThresholdExceeded	MosCQDS_ThresholdExceeded
RingBackResponseTime _ThresholdExceeded	IAJitterDS_ThresholdExceeded	RTPPacketLossDS_ThresholdExceeded
RegistrationResponseTime _ThresholdExceeded	JitterDS_ThresholdExceeded	

AverageLatency _ThresholdExceeded	Quality Dropped Below Threshold	

テストが実行され、正しく完了したかどうかを確認することができます。また、必要に応じてテストのトラブルシューティングを実行することもできます。これを行うには、次のオプションを選択します。 **[模擬テスト（Synthetic Tests）]** > **[IP SLA音声テスト（IP SLA Voice Test）]**。

[IP SLA 音声テスト（IP SLA Voice Test）] ページが表示されます。すべてのIP SLA 音声テストがページに表示されます。表の最後のカラムに各テストのステータスが表示されます。

表 *84 : IP SLA* 音声テスト ステータスの定義

テストのステータス	説明
Running	テストはアクティブで、データを収集中です。
Config Pending	デバイスが応答していないか、テストの設定中です。
Delete Pending	テストが削除される前の中間的な状態です。テストにアクションを実行できません。
Suspended	テストは一時停止され、データ収集やポーリングは行われていません。この状態は、デバイスが一時停止されたことによって発生します。
スケジュール済み	テストの作成またはアップデート後に表示されます。このステータスは、最初のポーリング サイクルで Running に変更されます。
Dormant	テストはアクティブですが、現在データを収集していません。テストは、各ポーリング サイクルの間で Dormant 状態になります。
Config Failed	テストは正しく設定されていません。デバイスのクレデンシャルが間違っているかデバイスのメモリ不足が問題となっている可能性があります。

IP SLA 音声テスト データ

Cisco Prime Collaboration Assurance は、テストの収集データをディスクに保存します。

次のトピックでは、データを使用し、データの安全を保護し、追加のテストを実行するための準備として必要な情報について説明します。

IP SLA 音声テスト データの保存

IP SLA 音声テスト のデータは、Cisco Prime Collaboration Assurance サーバの */opt/emms/cuom/data/N2Ntests* フォルダに保存されます。IP SLA 音声テストのデータは 30 日間保持されます。データ ストレージ ディレクトリには、次の 2 種類のファイルが保存されています。

- YYYYMMDD.csv：テストデータ。各ファイルには複数のレコードが入っています。各レコードはカンマ区切り形式（CSV）レコードで、ファイルにはポーリング間隔ごとに1つのレコードがあります。
- StudyInfo.log：テスト名、説明、ポーリング間隔、デバイス、開始日、終了日、操作の種類、ポーリング間隔、ステータスが含まれるログ。
-

IP SLA 音声テストのすべての設定情報は、IPSLATestInfo.log ファイルで取得できます。

IP SLA 音声テスト データの維持

テスト データを維持するには、次のすべてのタスクを実行する必要があります。

- **テスト データを保存するための十分なディスク容量があることを確認する**：テストの実行スケジュールの前にディスク スペースをチェックします。Cisco Prime Collaboration Assurance によって、テストのログ ファイルにデータが追加されます。テストの実行中、Cisco Prime Collaboration Assurance は、1 日に実行するテストごとに 1 つのデータ ファイルを生成します。直前のテストで使用されたスペースを算出して、見積もりを出してください。

  たとえば、ポーリング サイクルが 16 時間でサンプリング間隔が 1 分のテストでは、1 日におよそ 60 ～100 KB が使用されます。ポーリング サイクルが 16 時間、サンプリング間隔が 1 分、およびホップ数が 12 の Path Echo テストでは、1 日におよそ 1.2 MB が使用されます。

- **テスト データをエクスポートして保存する**。Cisco Prime Collaboration Assurance は、31 日が経過したすべてのデータ ファイルを消去します。31日より長くデータを保持するには、テストを別のサーバに保存する必要があります。

- **テスト データをバックアップする**。Cisco Prime Collaboration Assurance は、テスト データを Data Storage Directory に書き込み、[テストの詳細（Test Details）] ウィンドウに表示します。ファイルシステムのバックアップと同じ方法を使用して、定期的にバックアップを実行してください。

- **データを別のサーバにコピーするタイミングを決める**。テストデータは、別のサーバにコピーしてから検査する必要があります。

- **データを表示し、使用する**。テストの結果は、テストデータを Microsoft Excel にインポートしてから、またはサードパーティ製のレポート生成ツールを使用して、分析することができます。

テストがRunning状態の間は、テストデータのファイルに対して排他的な読み取り専用ロックするアプリケーションを使用してファイルを開かないでください。テスト データ ファイルがロックされている場合、Cisco Prime Collaboration Assurance は、出力データを書き込むことができないため、エラーをログ ファイルに書き込みます。

排他ロックするアプリケーションには、Microsoft Excel や Microsoft Word などがあります。テストが実行されていないときには、これらのアプリケーションを使用できます。

別のサーバへのテスト データのコピー

テスト データは、別のサーバにコピーしてから検査する必要があります。また、テスト データの別のサーバへのコピーは、バックアップ手段としても必要になる場合があります。テスト データは ASCII 形式です。別のサーバへのコピーは、SSH やコピー アンド ペーストなど、使用可能な任意の方法で実行することができます。

テスト データのファイルは、Data Storage Directory からコピーします。テスト データは CSV ファイルに書き込まれるため、テスト データ ファイルの名前は末尾が .csv になっています。

データ形式

Echo テスト データ レコード形式は、次のタイプのテストのエンドツーエンドの統計をキャプチャします。

- ICMP エコー
- UDP エコー
- Gatekeeper Registration Delay

表 *85 : Echo* テスト データ形式

フィールド番号	フィールド ID	内容	説明	値
1	Record ID	nnn	レコード タイプ 200	200
2	日付	yyyymmdd	カレンダー日付	例：20070201
3	タイム スタンプ	hhmmss	壁時計時刻	例：230000
4	完了時刻	番号	ラウンドトリップ時間（RTT）（ミリ秒）	0 ～ 4294967295 の間

5	完了ステータス	番号	次の数字のいずれかです。 • 1：OK • 2：切断 • 3：overThreshold • 4：タイムアウト • 5：ビジー • 6：notConnected • 7：ドロップ • 8：sequenceError • 9：verifyError • 10：applicationSpecific • 11：dnsServerTimeout • 12：tcpConnectTimeout • 13：httpTransactionTimeout • 14：dnsQueryError • 15：httpError • 16：エラー	1 ～ 16 の間
6	アプリケーション固有の完了ステータス	番号	（任意）完了ステータスが applicationSpecific (10) に設定された場合にだけ有効な、アプリケーション固有のステータス。	1001 ～ 2147483647 の間
7	ステータスの説明	番号	（任意）完了ステータスが applicationSpecific (10) に設定されている場合の完了ステータスの説明。デフォルト値はブランクです。	ASCII 文字
8	なし	ヌルインジケータ	未使用	*
（注） フィールド 9 ～ 37 には使用されず、null インジケータ（*）が含まれます。				
38	テスト名	テキスト	IP SLA 音声テストの名前	Sjc-VGtest

Ping Path Echo レコード形式は、Ping Path Echo テストに関するホップバイホップの統計をキャプチャします。テストでは発信元から宛先へ情報を記録します。

表 *86 : Ping Path Echo* テストのホップバイホップ統計のデータ形式

フィールド番号	フィールド ID	内容	説明	値
1	Record ID	nnn	レコード タイプ 201	201
2	日付	yyyymmdd	カレンダー日付	例：20070201
3	タイム スタンプ	hhmmss	壁時計時刻	例：230000
4	完了時刻	番号	ラウンドトリップ時間（RTT）（ミリ秒）	0 ～ 4294967295 の間
5	ホップ ID	番号	学習によって選択され、このパス上のホップに付与された一意の ID。	最大値は 30
6	ホップ アドレス	文字列	ホップの IP アドレス。	ASCII 文字

7	完了ステータス	番号	次の数字のいずれかです。 • 1：OK • 2：切断 • 3：overThreshold • 4：タイムアウト • 5：ビジー • 6：notConnected • 7：ドロップ • 8：sequenceError • 9：verifyError • 10：applicationSpecific • 11：dnsServerTimeout • 12：tcpConnectTimeout • 13：httpTransactionTimeout • 14：dnsQueryError • 15：httpError • 16：エラー	1 ～ 16 の間
8	アプリケーション固有の完了ステータス	番号	（任意）完了ステータスが applicationSpecific (10) に設定された場合にだけ有効な、アプリケーション固有のステータス。	1001 ～ 2147483647 の間
9	ステータスの説明	テキスト	（任意）完了ステータスが applicationSpecific (10) に設定されている場合の完了ステータスの説明。デフォルト値はブランクです。	ASCII 文字
10	なし	ヌル インジケータ	未使用	*
（注） フィールド 11 ～ 37 には使用されず、null インジケータ（*）が含まれます。				
38	テスト名	テキスト	IP SLA 音声テストの名前	Sjc-VGtest

このレコード形式では、Ping パス エコー テストのエンドツーエンドの統計情報をキャプチャします。テストは発信元から宛先に対して行われます。

表 *87 : Ping Path Echo* テストのエンドツーエンド統計のデータ形式

フィールド番号	フィールド ID	内容	説明	値
1	Record ID	nnn	レコード タイプ 204	204
2	日付	yyyymmdd	カレンダー日付	例：20070201
3	タイム スタンプ	hhmmss	壁時計時刻	例：230000
4	完了時刻	番号	ラウンドトリップ時間（RTT）（ミリ秒）	0 ～ 4294967295 の間
5	ホップ ID	番号	学習によって選択され、このパス上のホップに付与された一意の ID。このレコードでは、ホップ ID は常に 1 です。	1
6	ホップ アドレス	文字列	必須：宛先の IP アドレス。	ASCII 文字

7	完了ステータス	番号	次の数字のいずれかです。 • 1：OK • 2：切断 • 3：overThreshold • 4：タイムアウト • 5：ビジー • 6：notConnected • 7：ドロップ • 8：sequenceError • 9：verifyError • 10：applicationSpecific • 11：dnsServerTimeout • 12：tcpConnectTimeout • 13：httpTransactionTimeout • 14：dnsQueryError • 15：httpError • 16：エラー	1 ～ 16 の間
8	アプリケーション固有の完了ステータス	番号	（任意）完了ステータスが applicationSpecific (10) に設定された場合にだけ有効な、アプリケーション固有のステータス。	1001 ～ 2147483647 の間
9	ステータスの説明	テキスト	（任意）完了ステータスが applicationSpecific (10) に設定されている場合の完了ステータスの説明。デフォルト値はブランクです。	ASCII 文字
10	なし	ヌル インジケータ	未使用	*
（注） フィールド 11 ～ 37 には使用されず、null インジケータ（*）が含まれます。				
38	テスト名	テキスト	IP SLA 音声テストの名前	Sjc-VGtest

ジッタ MOS、ICPIF、および処理されたデータのレコード形式は、MOS と ICPIF の値、および処理されたジッタ統計値を保存します。

表 *88 :* ジッタ *MOS*、*ICPIF*、および処理されたデータのレコード形式

フィールド番号	フィールド ID	内容	説明	値
1	Record ID	205	必須：レコード タイプ 205	205
2	日付	yyyymmdd	カレンダー日付	例：20070201
3	タイム スタンプ	hhmmss	壁時計時刻	例：230000
4	ICPIF	番号	必須：ICPIF 値	
5	IP SLA 音声品質	番号	必須：MOS 値	例：3.6
6	発信元から宛先方向のパケット損失	番号	必須：パケット数	任意の正の整数。正の整数は 32 ビットにする必要があります。
7	宛先から発信元方向でのパケット損失	番号	必須：パケット数	任意の正の整数。正の整数は 32 ビットにする必要があります。
8	発信元から宛先方向でのジッタ	番号	必須：ミリ秒	0 以上で、100 以下
9	宛先から発信元方向でのジッタ	番号	必須：ミリ秒	0 以上で、100 以下
10	平均遅延	番号	必須：ミリ秒	0 以上で、100 以下
11	なし	ヌル インジケータ	未使用	*
（注） フィールド 12 ～ 37 には使用されず、null インジケータ（*）が含まれます。				
38	テスト名	テキスト	IP SLA 音声テストの名前	Sjc-VGtest

バッチ テストの作成

バッチ テストによって、事業所の状態と接続をテストできます。バッチ テストは、事業所に展開された音声アプリケーション（Cisco Unified Communications Manager Express や Cisco Unity Express など）で実行する一連の模擬テストと事業所の実際の電話で実行する一連の電話テストから構成されます。バッチテストを 1 日に 1 回実行するように設定すると、支社の音声ネットワークの状態を確認できます。

バッチ テストを 1 日に 1 回実行して、音声ネットワークの状態を確認できます。

バッチ テストは、XML ファイルをインポートして作成できます。バッチ テストはそれぞれ、複数の模擬テストおよび電話テストで構成されます。

Cisco Prime Collaboration リリース 12.1 SP1 以降の場合

1. 2 つの異なる合成テストでは、同じセキュア JTAPI ユーザ ID とインスタンス ID を使用することはできません。
2. 合成テストに設定されている JTAPI ユーザは、CUCM の管理で使用するものと同じものは使用できません。

バッチ テストを作成するには、次のようにします。

始める前に

- シード ファイルの形式が正しいことを確認します。インポート ファイル形式の詳細については、「バッチ テスト インポート ファイルの形式」を参照してください。

ステップ 1 選択 **[模擬テストセンター（Synthetic Test Center）]** > **[バッチテスト（Batch Test）]**。

Cisco Prime Collaboration リリース 11.5 以降の場合

移行方法 **[模擬テストセンター（Synthetic Test Center）]** > **[バッチテスト（Batch Test）]**。

ステップ 2 [作成（Create）] をクリックします。

ステップ 3 シード ファイルを参照して、[OK（OK）] をクリックします。

バッチ テストのスケジュール時刻および日付はインポート ファイルで設定します。ただし、オン デマンド バッチ テストを実行する場合は、[Run Now] ボタンを使用して実行できます。

バッチ テスト インポート ファイルの形式

バッチテストのインポートファイルは、XML ファイルです。インポートファイルのサンプル（batchtest.xml）が、*/opt/emms/cuom/ImportFiles* ディレクトリにあります。

1 つのバッチテストインポートファイルに 1 つのバッチテストの情報が記録されます。各バッチ テスト インポート ファイルには、特定のバッチテストのSynthetic Test の前提条件および

Phone Test：Batch および On Demand Testを設定するために必要なすべての情報が含まれています。

バッチ テスト インポート ファイルを作成するときは、次に示す各フィールドのガイドラインに従ってください。

- TestSchedule：複数のスケジュール エントリを指定できます。
- 各 ScheduleEntry：次の 5 つのフィールドが必須です。
  - Month：サポートされていません。
  - DayOfMonth：サポートされていません。
  - DayOfWeek：0 ～ 6 の範囲で指定します。すべての曜日を指定するには、アスタリスクを使用します。
  - Hour：0 ～ 23 の範囲内でなければなりません。
  - Minute：0 ～ 59 の範囲内でなければなりません。
- CallAgent：Cisco Unified Communications Manager または Cisco Unified Communications Manager Express を指定できます。
- PhoneMACAddress：模擬電話の MAC アドレス。00059A3B7700 ～ 00059A3B8AFF の範囲内でなければなりません。

（注） ソフト フォンの MAC アドレス フィールドにデバイス名が表示されます。

- PhoneProtocol：模擬電話のプロトコル。SCCP または SIP です。
- PhoneURIorExtension：SIP 電話の内線番号または URI です。これは、SCCP 電話の場合は無視されます。
- OnsiteAlertNumber：IsOSANEnabled が true に設定されている場合にだけ必須です。
- DialingNumber：省略可能。入力が存在しない場合は PhoneNumber が使用されます。このフィールドが有効なのは、クラスタ間コールの場合だけです。発信元電話機から別のクラスタにある発信先電話機に電話をかけるためにダイヤルする必要のある番号全体を入力しなければなりません。

  たとえば、電話番号のみ、またはダイヤル パターン/アクセス ディジットと電話番号です。

既存のバッチ テストを変更するには、新しいバッチ テスト インポート ファイルをインポートします。それまでのバッチ テスト情報は、新しいインポート ファイルによって上書きされます。インポートファイルを変更するには、手動でファイルを編集する必要があります。

Batch Test の管理

次の表に、[バッチテスト（Batch Test）] ページから実行できるタスクを示します。

タスク	説明
バッチテストの詳細の表示	[Test Details] ページには、特定のバッチ テストに関するすべての詳細情報が表示されます。このページには、バッチ テストの一部である Synthetic Test と Phone Test：Batch および On Demand Test がすべて表示されます。
バッチ テストの編集	複数のテストを編集するには、次のオプションを選択します。 **[模擬テストセンター（Synthetic Test Center）] > [バッチテスト（Batch Test）]**。[バッチテスト（Batch Tests）] ページで、変更するバッチ テストを選択し、[編集（Edit）] をクリックします。
テストのステータスを確認する	テストが実行され、正しく完了したかどうかを確認することができます。また、必要に応じてテストのトラブルシューティングを実行することもできます。 テストのステータスを確認するには、次のオプションを選択します。 **[模擬テストセンター（Synthetic Test Center）] > [バッチテスト（Batch Test）]**。 [バッチテスト（Batch Tests）] ページが表示されます。現在のすべてのバッチテストがページに表示されます。表の最後のカラムに各テストのステータスが表示されます。 • [実行中（Running）] : テストがアクティブになり、データが収集されます。 • [中断（Suspended）] : テストは、データの収集またはポーリングの状態から中断されます。この状態は、デバイスが一時停止されたことによって発生します。 • [スケジュール済み（Scheduled）] : テストの作成または更新後に表示されます。このステータスは、最初のポーリング サイクルで Running に変更されます。

タスク	説明
バッチ テストを中断または再開する	バッチテストを一時停止すると、それ以降はスケジュールされた時刻には実行されなくなります。テストがシステムから削除されることはありません。テストを取り消す場合は、テストを削除する必要があります。 一時停止して、一括テストを再開するには、次のオプションを選択します。 **[模擬テストセンター（Synthetic Test Center）] > [バッチテスト（Batch Test）]**。 [Batch Tests] ページが表示されます。 • バッチ テストがアクティブな場合に実行を停止するには、[中断（Suspend）] をクリックし ます。 • バッチテストが中断中にスケジュールされた時刻に実行する場合は、[再開（Resume）] をクリックし ます。 バッチ テストを実行するスケジュールの日時は、インポート ファイルで設定します（「（IP SLA 音声テスト）のインポート ファイルの形式」を参照してください）。ただし、バッチテストをオンデマンドで実行する場合は、[今すぐ実行（Run Now）] ボタンを使用して実行できます。

タスク	説明
バッチ テスト結果の表示	バッチテストのコンポーネントが不合格になっても、イベントは生成されません。バッチ テストの結果は、[Batch Test Results] レポートで確認する必要があります。各バッチテストの新しい [Batch Test Results] レポートが 24 時間間隔で生成されます。 Cisco Prime Collaboration Assurance では、バッチ テストによって収集されたデータが、*/opt/emms/cuom/data/bt* フォルダー内の Cisco Prime Collaboration Assurance サーバに保存されます。 [Batch Test Results] レポートには、バッチ テスト全体に関する次の情報が表示されます。 • テストのステータス • テストの開始日時と完了日時。 [Batch Test Results] レポートには、バッチ テストを構成する個々のテストに関する次の情報が表示されます。 • テストの種類。 • ネガティブ テストであるかどうか。 • テストのステータス（合格または不合格）。 • テストが終了した日時。 • エラー メッセージ（ある場合）。 テスト結果を表示するには、次のオプションを選択します。 **[模擬テストセンター（Synthetic Test Center）]** > **[バッチテスト（Batch Test）]**。[バッチテスト（Batch Tests）] ページで、結果を表示するバッチ テストを選択し、[結果（Results）] をクリックします。
バッチ テスト結果の印刷	バッチ テスト レポートで、ページの右上隅にあるプリンタ アイコンをクリックします。
バッチ テスト結果のエクスポート	テスト結果をクライアント システムに保存するには、エクスポート機能を使用します。 バッチ テストの結果をエクスポートするには、次の手順を実行します。 **1.** バッチ テスト レポートで、ページの右上隅にあるエクスポート アイコンをクリックします。 **2.** エクスポートする **CSV** または **PDF** のいずれかのフォーマットを選択し、[OK] をクリックします。

タスク	説明
バッチ テストの削除	一括テストを削除するには、次のオプションを選択します。**[模擬テストセンター（Synthetic Test Center）] > [バッチテスト（Batch Test）]**。[バッチテスト（Batch Tests）] ページで、変更するバッチ テストを選択し、[削除（Delete）] をクリックします。

Phone Test：Batch および On Demand Test

バッチ テストやオンデマンド テストの一部として実行される電話テストは、ネットワーク内の実際の電話機を制御して、その電話機から別の電話機に電話をかけるというものです。電話テストでは、JTAPI クレデンシャルが使用されます。

Cisco Prime Collaboration Assurance で電話テスト機能を適切に動作させるには、Cisco Unified CM で JTAPI クレデンシャルを設定する必要があります。

電話テストを作成する際は、次のガイドラインに従ってください。

- テスト フォンとテスト プローブは、同じ Cisco Prime Collaboration Assurance に属する必要があります。これは、JTAPI を使用し、Cisco Unified CM を介してこれらの電話機とプローブを制御するためです。テスト フォン（テスト対象の電話機）とテスト プローブ（テストの実行に使用した電話機）が別の Cisco Unified CM に属する場合、テストは失敗します。
- コール テストのタイプがクラスタ間コールである場合だけは、宛先電話機が別の Cisco Unified CM に属していてもかまいません。この場合、ユーザは、宛先 Cisco Unified CM のクレデンシャルを XML ファイルに指定する必要があります。
- 電話テストを実行する前に、Cisco Unified CM での設定が正しいことと、さまざまな電話操作が機能していることを、実際の電話機を使用して確認してください。

（注） これらの電話テストは、その他の Cisco Prime Collaboration Assurance 電話テスト（合成テストや電話ステータス テスト）と間違わないでください。ここに示す電話テストはバッチ テストの一部として作成されるものであり、オンデマンドで IP Phone レポートから起動することも可能です。これらのテストは、実際の電話機を制御しながら実行されます。

次の表には、さまざまな種類の電話テストが示されています。

表 *89 :* 電話テストの説明：バッチ/オンデマンド テスト

テスト	説明
コール保留	2 台の電話機を制御して次のことを実行します。 **1.** 電話機 A から電話機 B にコールを発信する。 **2.** 電話機 B でコールを保留にする。 **3.** コールを切る。
コール転送	3 台の電話機を制御して次のことを実行します。 **1.** 電話機 A から電話機 B にコールを発信する。 **2.** コールを電話機 B から電話機 C に転送する。 **3.** コールが電話機 C で受けられたことを確認する。 **4.** コールを切る。
コール パーク	3 台の電話機を制御して次のことを実行します。 **1.** 電話機 A から電話機 B にコールを発信する。 **2.** 電話機 B でコール パークを行う。 コールは電話機 B からは削除され、どの番号にコール パークされているかを伝えるメッセージが表示されます（たとえば「Call Park at 80503」）。 **3.** 電話機 C から、コール パーク番号にダイヤルする。 パークされたコールが、ダイヤルした電話機に転送される。 **4.** コールを切る。

テスト	説明
コール会議	3 台の電話機を制御して次のことを実行します。 **1.** 電話機 A から電話機 B にコールを発信する。 **2.** 電話機 A から電話機 C にコールを発信して電話会議に追加する。 **3.** コールを切る。
コール転送	3 台の電話機を制御して次のことを実行します。 **1.** 電話機 A から電話機 B にコールを発信する。 **2.** 電話機 B から電話機 C にコールを転送する。 **3.** 電話機 C がコールを受ける。 **4.** コールを切る。
コール テスト	1 台の電話機を制御して、指定された番号にコールを発信します。これは、実際の電話機から特定の番号へのコールでもかまいません。この場合は、テストで制御されるのは発信側だけです。 または、実際の電話機から別の実際の電話機にかけることもできます。この場合は、テストで発信側と受信側の両方が制御されます。

Phone Test on Demand の作成

[IP Phones/Lines] レポートで電話機を選択して、電話テストを表示してオンデマンドで実行することができます。選択された電話は同じ Cisco Unified CM に属する必要があります。電話テストでは、JTAPI クレデンシャルが使用されます。JTAPI クレデンシャルは、Unified CM で設定する必要があります。

JTAPI の電話テストでは、この形式の内線番号を使用する E.164（"+"）ダイヤルと電話をサポートしています。

電話テストを作成するには、次のオプションを選択します。 **[模擬テストセンター（Synthetic Test Center）] > [音声電話機の機能テスト（Audio Phone Features Test）]**。

Cisco Prime Collaboration リリース 11.5 以降の場合

移行方法 **[模擬テスト（Synthetic Tests）] > [音声電話機の機能テスト（Audio Phone Features Test）]**。

次の表に、オンデマンドの電話テストの作成中に選択可能なフィールドを示します。

表 *90 :* 電話テストの説明：バッチ/オンデマンド テスト

項目	説明
Ciscoユニファイド コミュニケーション マネージャ	電話レポートから選択された電話の Unified CM を一覧表示します。左側のペインから Unified CM を選択し、[>>] ボタンをクリックして、Unified CM フィールドに追加することもできます。以前のテスト電話とヘルパー電話の選択はクリアされるため、再度指定する必要があります。
[JTAPI Username] と [JTAPI Password]	Unified CM で構成されている JTAPI ユーザ名とパスワードを入力します。
Test Phones	[Test Phones] に電話機を追加するには、次の手順に従います。 **1.** [電話レポートから追加（Add from Phone Report）] をクリックします。 **2.** [電話レポート（Phone Report）] ウィンドウで、追加する電話を選択し、[選択（Select）] をクリックします。 追加された電話は、このテストの最初に提供された同じ Cisco Unified CM に属している必要があります。 電話を 1 台だけ選択したときに、その電話機の内線番号が [Personalized Report] 内の他の電話機と共有されている場合は、生成されるレポートにはすべての電話機（選択された電話機も含む）に関する詳細情報が表示されます。
Helper Phones	[Helper Phones] に電話機を追加するには、次の手順に従います。 **1.** [電話レポートから追加（Add from Phone Report）] をクリックします。 **2.** 追加する電話機を選択して [選択（Select）] をクリックします。 追加された電話は、このテストの最初に提供された同じ Cisco Unified CM に属している必要があります。 電話を 1 台だけ選択したときに、その電話機の内線番号が [Personalized Report] 内の他の電話機と共有されている場合は、生成されるレポートにはすべての電話機（選択された電話機も含む）に関する詳細情報が表示されます。

Phone Tests	どの電話テストの結果を表示するかを選択します。電話テストの説明：バッチ テストおよびオンデマンド テスト [コール テスト（Call Test）] が選択されている場合、[コールタイプ（Call Type）]、[合格基準（Success Criterion）]、[電話番号（Phone Number）] のフィールドが有効になります。
コール タイプ	ドロップダウン リストからコールのタイプを選択します。[クラスタ間コール（Inter Cluster Call）] を選択すると、次のフィールドが有効になります。[Cisco Unified Communications Manager JTAPI ユーザ名と JTAPI パスワード（Cisco Unified Communications Manager JTAPI Username JTAPI Password）]。
Success Criterion	ドロップダウン リストから合格基準を選択します。
Phone Number	コールテストのためにダイヤルされる発信先電話番号を、このフィールドで指定する必要があります。
Dialing Number	[Call Type] で [Inter Cluster Call] が選択されているときは、発信元電話機から別のクラスタにある発信先電話機に電話をかけるためにダイヤルする必要のある電話番号全体を入力します。この番号には、ダイヤル パターンやアクセス番号が含まれることもあります（たとえば「94151234567」）。このフィールドは必須ではありません。空白にした場合、電話番号フィールドが代わりに使用されます。
Ciscoユニファイド コミュニケーション マネージャ	[コール タイプ（Call Type）] として [クラスタ間コール（Inter Cluster Call）] を選択した場合、[電話番号（Phone Number）] フィールドで指定した電話番号で使用する Cisco Unified CM を入力します。
[JTAPI Username] と [JTAPI Password]	[コール タイプ（Call Types）]で[クラスタ間コール（Inter Cluster Call）] を選択した場合は、前のフィールドに記載されている Cisco Unified CM のユーザ名とパスワードを入力します。

Audio Phone Features Test

Audio Phone Features Test ポートレットには、すべての Cisco Unified Communications Manager ノードでの電話機テストの概要が表示されます。

次の詳細を提供します。

- テストされた電話の台数
- テストされる機能のリスト
- テストを最後に実行した日付と時刻
- 最新の電話テストの結果
- 顧客名（MSP モードのみ）

電話機能テストには、次の要件があります。

- **JTAPI ユーザ（アプリケーション ユーザ）の要件**：

標準権限	権限に対する特権およびリソース
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。
Standard CCM Admin Users	Cisco Unified Communications Manager Administration へのログイン権限を付与します。
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 CTI 対応	CTI アプリケーションの制御を可能にします。
Standard CTI Allow Call Monitoring	CTIアプリケーションまたはデバイスでコールを監視できます。
[標準 CTI による接続時の転送および会議をサポートする電話の制御（Standard CTI Allow Control of Phones supporting Connected Xfer and conf）]	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 によるすべてのデバイスの制御（Standard CTI Allow Control of All Devices）	CTI で制御可能なすべてのデバイスを制御できます。

（注）

- 「Standard CTI Allow Control of all devices」 は、他の CTI Standard ロールを置き換えるためのオプショナル ロールです。このロールは、専用の JTAPI テスト ユーザが作成されている場合のみ推奨されます。
- すべてのテストする電話機は、アプリケーション ユーザの一覧で制御されている必要があり、すべてのユーザがすべての Unified CM ノードに存在する必要があります。
- **Cisco Prime Collaboration リリース 12.1 SP1 以降の場合**
  1. 2 つの異なる合成テストでは、同じセキュア JTAPI ユーザ ID とインスタンス ID を使用することはできません。
  2. 合成テストに設定されている JTAPI ユーザは、CUCM の管理で使用するものと同じものは使用できません。

- **電話機の要件**：
  - [標準CTIを有効にする（Standard CTI Enabled）]
  - すべてのテスト ユーザを同じサブスクライバ（または Unified CMノード）に登録する
  - 電話機が Cisco Prime Collaboration Assurance で [Managed] 状態にある
  - 電話機は、電話機の選択時に使用する Phone Report の Management Status Reason で、「AllFine」 として一覧表示されている必要がある
- **プロセッサの要件**：
  - JTAPI クレデンシャルを使用し、Unified CM に対して有効なテストである
  - テスト ノードで CTI Manager を実行する
  - テスト ノードで AXL Web Services を実行する
  - クラスタ ID は、各クラスタの各 Unified CM ノードで一意に設定されている必要がある
  - プロセッサが Cisco Prime Collaboration Assurance で [Managed] 状態にある
- **Secure JTAPI の要件**

（注）

Cisco Prime Collaboration リリース 12.1 SP1 以降の場合

1. 合成テストに設定されている JTAPI ユーザは、CUCM の管理で使用するものと同じものは使用できません。
2. 2 つの異なる合成テストでは、同じセキュア JTAPI ユーザ ID とインスタンス ID を使用することはできません。

表 *91 : Secure JTAPI* フィールドの説明

フィールド名	説明
JTAPI Cisco Unified CM からセッション ステータス情報を取得する際に使用します。	

フィールド名	説明
	安全なJTAPI（TLS1.2）接続を確立するため、JTAPI 固有の新しいパラメータ セットが導入されました。 JTAPI 固有のパラメータ セットは、次のとおりです。 1. **JTAPI ユーザ名**： Unified Communications Managerに設定されたJTAPIユーザ名を指定します。 2. **JTAPI パスワード**：Cisco Unified Communications Manager で設定されたJTAPI パスワードを指定します。 3. **Secure JTAPI** チェックボックス： 1. **チェックボックスをオンにする**：このオプションをオンにすると、Cisco Unified Communications Managerへのセキュアな TLS 接続が有効になります。 （注） “Standard CTI Secure Connection” ロールが、他の必要なロールとともに、このJTAPI ユーザと関連付けられていることを確認します。 2. **チェックボックスをオフにする**：このチェックボックスをオフにすると、JTAPIはセキュアな接続を確立できません。 （注） このJTAPI ユーザに関連付けられている “Standard CTI Secure Connection” ロールが削除されていることを確認します。[Monitor Conferences] へと続行するには、必要な役割が設定されていることを確認します。 詳細については、「Cisco Prime Collaboration Assurance用のデバイスをセットアップ」を参照してください。

フィールド名	説明
	チェックボックスを使用すると、新しい Secure JTAPI フィールドにパラメータを入力できます（有効または無効）。

フィールド名	説明

フィールド名	説明
	4. TFTP サーバ IP アドレス - TFTP サーバの IP アドレスを指定します。 （注） この値は、CUCM クラスタのいずれかのノードである必要があります。そのノードで、TFTP サービスが実行されていることを確認します。 **5. TFTP サーバ ポート**：TFTP サーバ ポートのデフォルト値は 69 です。 （注） システム管理者に推奨されない限り、デフォルト値は変更しないようにします。 **6. CAPF サーバ IP アドレス** - CAPF サーバの IP アドレスを指定します。 （注） 1. CTI、JTAPI、および TAPI アプリケーションを保護する方法の詳細や、Certificate Authority Proxy Function の詳細については、『Cisco Unified Communications Manager のセキュリティ ガイド』の「CTI、JTAPI、TAPI の認証と暗号化のセットアップ」および「Certificate Authority Proxy Function」の各章を参照してください。 2. CUCM で CAPF プロファイルを作成するときは、**[キーの順序（Key Order）]** ドロップダウンリストから **[RSA のみ（RSA Only）]** を選択してください。 3. CUCM Publisher IP アドレスは、常に指定する必要があります。 **7. CAPF サーバ ポート**：CAPF サーバ ポート番号のデフォルト値は 3804 です。 （注） 入力した値が、Cisco Unified Communication Manager で設定された値と一致していることを確認しま

フィールド名	説明
	す。 **8. パブリッシャ用のインスタンス ID** - このフィールドには、アプリケーションの CAPF 設定、または Cisco Unified Communication Manager クラスタのエンド ユーザ CAPF のプロファイル設定ページで設定した、アプリケーション インスタンスの識別子を指定します。 **9. セキュア認証文字列**：アプリケーションの CAPF 設定セクション、または各 Communication Manager Publisher のエンドユーザ CAPF のプロファイル設定ページで設定した認証文字列を入力します。 （注） 「セキュアな JTAPI 接続のトラブルシューティング」セクションには、考えられるエラーに対するトラブルシューティングの詳細や、Conference Diagnostics が捉えることのできない CUCM for Secure JTAPI and Sessions のセットアップで推奨されるアクションが一覧表示されます。

トラブルシューティング

Cisco Prime Collaboration Assurance にて、次の電話機能テストのシナリオでトラブルシューティングを実行します。

- **問題**

  電話機能テストが失敗し、次のエラー メッセージが表示されます。

  「アドレス XXXXXX がプロバイダのドメインにありません」

  推奨アクション

  - 機能テスト用に選択されたエンドポイントが、すべて同じ JTAPI ユーザに割り当てられていることを確認します
  - JTAPI ユーザで、「[すべてのデバイスで Standard CTI 許可を制御する」」ロールが選択されていることを確認します。

- **問題**

  電話機能テストが失敗し、次のエラー メッセージが表示されます。

  「プロバイダを作成できずに接続が拒否される」

推奨アクション

- ユーザの JTAPI クレデンシャルが Unified CM で設定されていることを確認します
- 機能テストで使用されている電話機が、同じJTAPIユーザに割り当てられていることを確認します
- CTI Manager がアクティブで、テストに使用する Unified CM ノードが実行されていることを確認します
- Unified CM の JTAPI 実装が変更されている場合は、Cisco Prime Collaboration Assurance JTAPI Java Archive（JAR）ファイルを更新します

CME 診断

CME 診断(**[診断（Diagnose）]** > **[CME診断（CME Diagnostics）]**）ページには、Cisco Unified Communications Manager Express（Cisco Unified CME）デバイスおよび関連付けられている Cisco Unity Express デバイスが表示されます。

Cisco Unified CME デバイスに対して、デバイス 360 ビューを起動することができます。

また、次の情報も表示されます。

- 各 CME に登録されている ephone の数。この数をクリックすると、[エンドポイントの診断（Endpoint Diagnostics）] ページをクロス起動できます。
- 登録解除された ephone 数。この数をクリックすると、[エンドポイントの診断（Endpoint Diagnostics）] ページをクロス起動できます。
- CME のアクティブなアラームと確認応答済みアラームの合計数。この数をクリックすると、[アラームとイベント（Alarms & Events）] ページの [アラーム（Alarms）] タブが開きます。
- CUE の CME 登録のステータス。CUE が CME に統合されていない場合、または CUE が Cisco Prime Collaboration Assurance で管理されていない場合、この列には N/A と表示されます。
- CUE のアクティブなアラームと確認応答済みアラームの合計数。

（注） [エンドポイントの診断（Endpoint Diagnostics）] ページの [エンドポイント名（Endpoint Name）] フィールドは、CME 電話機ではサポートされません。

制限事項

Cisco Prime Collaboration Assurance は、複数の OID（DN の 1.3.6.1.4.1.9.9.439.1.1.47.1.4 など）を使用して CME から電話情報を取得します。SIP 電話機は SNMP に応答しません。理想的には CLI アプローチ（net config を推奨）を使用する必要があります。

Cisco Prime Collaboration リリース 12.1 SP3 以降の場合

- Cisco Prime Collaboration Assurance は、複数の OID（DN の 1.3.6.1.4.1.9.9.439.1.1.47.1.4 など）を使用して CME 電話機から電話情報を取得します。
- Cisco Prime Collaboration Assurance では、CME 電話機からの SIP 電話機の検出はサポートされません。

Cisco Unified CME Syslog メッセージを使用した IP フォンの監視

1. CME に Cisco Prime Collaboration Assurance のIP 設定を追加して、Cisco Unified Communications Manager Express の syslog メッセージを正常に受信します。

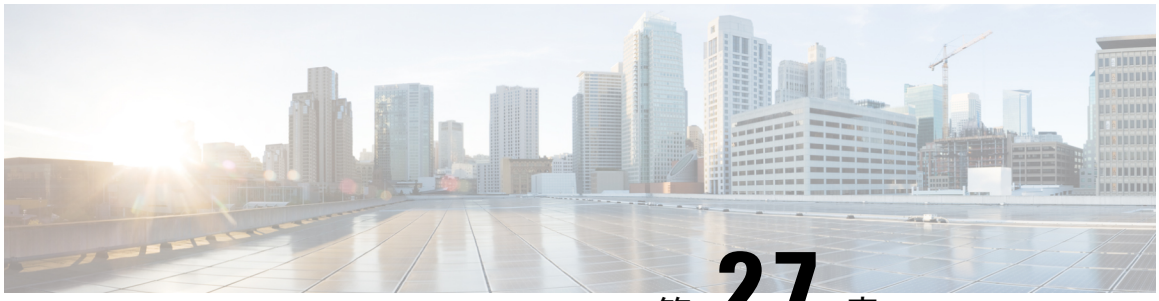
   ```
   CME #(config)# logging <PCA_IP>
   ```

2. Syslog が CME で設定されている場合、IP フォン登録または登録解除イベントを使用して、syslog メッセージを Cisco Prime Collaboration Assurance に送信します。
3. この例を使用して、IP フォン登録を設定します。

   エラー メッセージ

   ```
   %IPPHONE-6-REGISTER_NEW: ephone-3:SEP003094C38724 IP:1.4.170.6 Socket:1
   DeviceType:Phone
   ```

   が登録 されています。



第 27 章

ビデオ エンドポイントのトラブルシューティング ワークフロー

このセクションでは、次の点について説明します。

- ビデオ エンドポイントのトラブルシューティング ワークフロー （657 ページ）

ビデオエンドポイントのトラブルシューティングワークフロー

Cisco Prime Collaboration リリース 11.6 以降の場合

このセクションを確認する前に、Cisco Prime Collaboration Assurance の検出ワークフローを理解しておく必要があります。デバイスの検出プロセスの詳細については、『Cisco Prime Collaboration Assurance ガイド - Advanced, 11.x』の「デバイスの検出」セクションを参照してください。

トラブルシューティングのワークフローでは、[] [] ページで [システムステータスのポーリング間隔（System Status Polling Interval）]、[フロー統計のポーリング間隔（Flow Statistics Polling Interval）] に対して定義された値に基づいて、デバイスがポーリングされます。

トラブルシューティング ワークフロー中、エンドポイントおよび会議デバイスのステータスをチェックするため、それらのポーリングが 1 分間隔で行われます。

ネットワーク デバイスに関する詳細（CPU 使用率、メモリ使用率、インターフェイスなど）を表示できます。

（注） Cisco Prime Collaboration Assuranceを MSP モードで導入している場合、

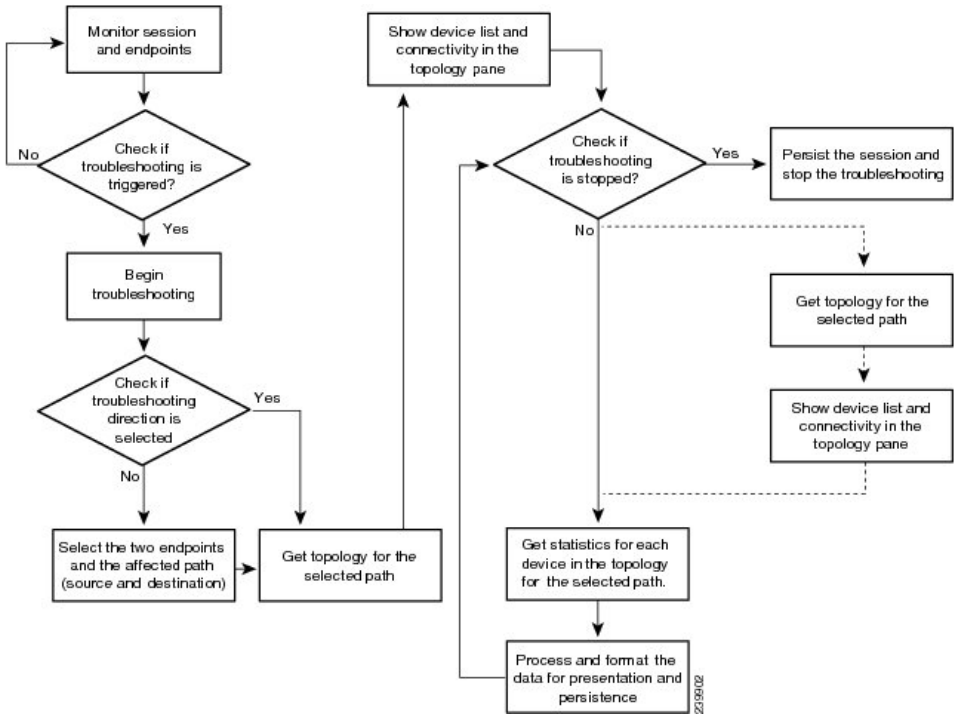
[会議（Conference）] のトラブルシューティングはサポートされません。

トラブルシューティング ワークフローは、Cisco Prime Collaboration Assurance システムのパフォーマンスに影響を与えます。ウォッチ リストに会議またはエンドポイントを追加するのは、必要な場合だけにしてください。

会議のトラブルシューティング ワークフローを次に示します。

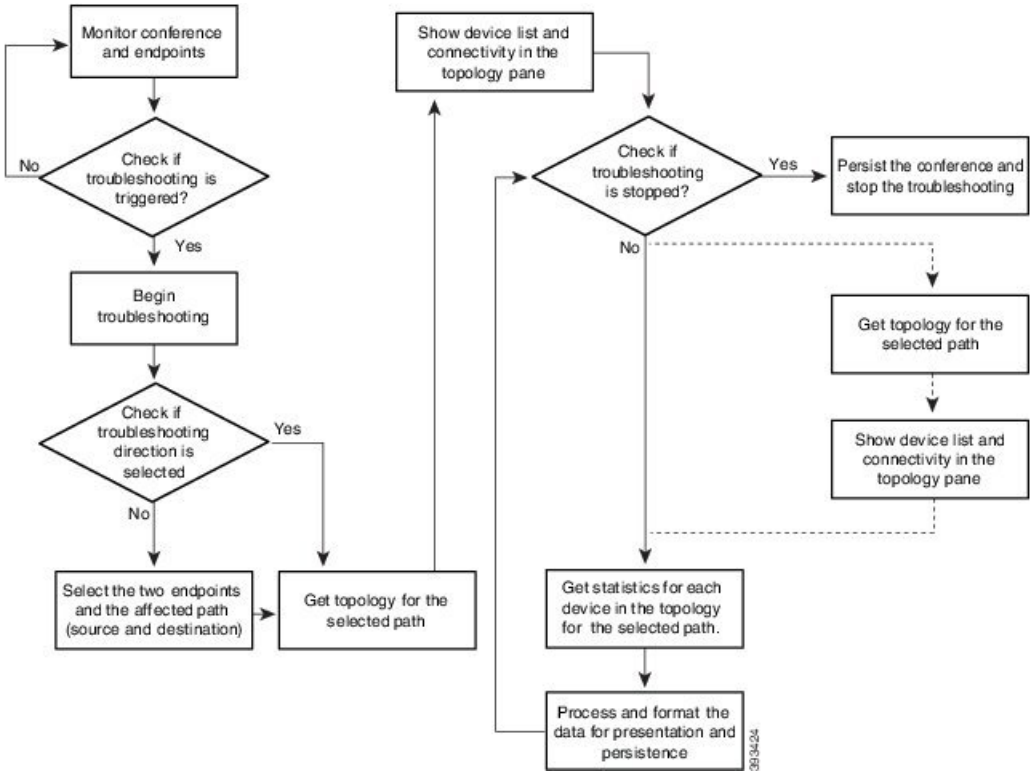
Cisco Prime Collaboration リリース 11.1 以前の場合

図 *9:* セッションのトラブルシューティング ワークフロー



Cisco Prime Collaboration リリース 11.6 以降の場合

図 *10* : 会議のトラブルシューティング ワークフロー



関連トピック

デバイスの検出

トラブルシューティング ワークフローの機能

次に、トラブルシューティング ワークフローの主な特徴を示します。

- トラブルシューティングは自動または手動で開始できます。
  - 自動トラブルシューティングは、会議を監視リストに追加すると起動されます。
  - 自動トラブルシューティングは、エンドポイントの1つが監視リストに含まれている場合に起動されます。トラブルシューティング ワークフローは、エンドポイントが監視対象状態になっている場合に限り開始できます。
  - 自動トラブルシューティングは、パケット損失、ジッター、または遅延アラームの値が定義済みのしきい値を超えると起動されます。これは、ポイントツーポイント会議のみに適用できます。
  - 自動トラブルシューティングは、パケット損失、ジッター、または遅延アラームがマルチポイント 会議で発生する場合は起動されません。
  - 手動トラブルシューティングは、[会議（Conference）] ページから開始できます。

会議およびエンドポイントのトラブルシューティング ワークフローを開始する方法の詳細については、「トラブルシューティング ワークフローの開始（664 ページ）」を参照してください。

- 2 つのエンドポイント間でパケット損失、ジッター、または遅延アラームが存在するとき、自動トラブルシューティングに対して設定されている場合はトラブルシューティング ワークフローが開始されます。このアラームがクリアされると、トラブルシューティング ワークフローは停止します。
- 双方向の 2 つのエンドポイントの間でトラブルシューティングがサポートされています。トラブルシューティング ワークフローを手動で開始する場合は、エンドポイント間のトラブルシューティングの方向を選択できます。
- エンドポイントと Cisco MSE との間ではトラブルシューティングがサポートされています。トラブルシューティングは、ビデオ エンドポイントから SBC への方向で行われ、その逆方向では行われません。
- エンドポイントと Cisco TelePresence Server との間ではトラブルシューティングがサポートされています。トラブルシューティングは、エンドポイントから Cisco TelePresence Server への方向で行われ、その逆方向では行われません。
- エンドポイントと Cisco MSE との間ではトラブルシューティングがサポートされています。トラブルシューティングは、エンドポイントから Cisco MSE への方向で行われ、その逆方向では行われません。
- エンドポイントと Cisco VCS との間ではトラブルシューティングがサポートされています。トラブルシューティングは、エンドポイントから Cisco VCS への方向で行われ、その逆方向では行われません。
- 状態が [Unknown] であるエンドポイントについては、既知のエンドポイントからこの不明なエンドポイントにトラブルシューティングできます。マルチポイント会議でも、同じ方法でトラブルシューティングを行うことができます。
- トラブルシューティング ワークフローは、開始時から最長 4 時間実行されます。トラブルシューティング ワークフローがこの時間内に終了しない場合は、Cisco Prime Collaboration Assurance はワークフローを自動的に終了します。
- 最大 50 個の同時トラブルシューティング ワークフローが一度に存在できます。使用できます。

  この制限を超えると、トラブルシューティング ログ ファイルにエラー メッセージが表示されます。

会議のトラブルシューティング ワークフローの機能

次に、スケジューリングされた会議が監視リストに追加された場合のトラブルシューティング ワークフローの主な動作を示します。

- 自動トラブルシューティング ワークフローは、監視リストに追加されるすべての会議で開始されます。

- マルチポイント会議では、トラブルシューティングは、エンドポイントが会議に参加するとすぐに開始されます。
- マルチポイント会議では、エンドポイントのトラブルシューティングが停止されると、トラブルシューティング ワークフローは、会議内の他のエンドポイントについて続行されます。このエンドポイントのトラブルシューティングは手動で開始する必要があります。
- マルチポイント会議では、問題が原因でエンドポイントが再開されると、会議への参加後に、このエンドポイントの新しいトラブルシューティング ワークフローが起動されます。会議内の他のエンドポイントに影響はありません。
- 監視リストから会議が削除されると、次の条件では、関連付けられたトラブルシューティング ワークフローは停止します。
  - その会議についてトリガーされたパケット損失アラーム、ジッターアラーム、および遅延アラームがない。
  - 手動で起動されたトラブルシューティング ワークフローがない。
- パケット損失、ジッター、または遅延アラームが原因でトラブルシューティング ワークフローが起動された場合は、次の条件では、パケット損失、ジッター、または遅延アラームがクリアされると、トラブルシューティング ワークフローは停止します。
  - 会議が監視リストに追加されていない。
  - 手動で起動されたトラブルシューティング ワークフローがない。
  - トラブルシューティング ワークフローを手動で停止した、または会議が終了した。
- 手動で起動したトラブルシューティング ワークフローは、手動で停止する必要があります。それ以外の場合は、会議が終了すると停止します。
- 会議を再度監視リストに追加すると、新しいトラブルシューティング ワークフローが開始されます。

エンドポイントのトラブルシューティング ワークフローの機能

トラブルシューティング ワークフローは、エンドポイントが監視対象状態になっている場合に限り開始できます。次に、エンドポイントが監視リストに追加された場合のトラブルシューティング ワークフローの主な動作を示します。

- エンドポイントの自動トラブルシューティングは、その会議に参加するとすぐに開始されます。（監視リストに追加された）エンドポイントに関連付けられた会議のトラブルシューティング ワークフローを停止できます。この会議のトラブルシューティングは手動で開始する必要があります。
- 会議中に、エンドポイントが監視リストから削除されると、そのエンドポイントのトラブルシューティングは停止します。

- 会議および関連付けられたエンドポイントが管理リストに属している場合に、エンドポイントが監視リストから削除されると、そのセッションのトラブルシューティング ワークフローは、会議が終了するまで続行されます。
- 会議および関連付けられたエンドポイントが監視リストに属している場合は、会議が監視リストから削除されると、そのエンドポイントのトラブルシューティング ワークフローは、エンドポイントが会議から切断されるまで続行されます。つまり、会議とエンドポイントが監視リストに属している場合は、エンドポイントにより高い優先順位が付けられます。
- MRA エンドポイントでは、トラブルシューティング用の脚は表示されません。非 MRA エンドポイントでは、トラブルシューティング ワークフローは、Cisco Collaboration Edge を使用して、エンドポイントから Cisco VCS に対して行われます。

発信元と宛先のエンドポイントをトラブルシューティングするためのサポートマトリクス

次の表には、発信元エンドポイントと宛先エンドポイントの間のトラブルシューティング サポートの詳細を示してあります。

Cisco Prime Collaboration リリース 11.5 以前の場合

（注）
- マルチポイント コールでトラブルシューティングを実行する場合は、ソース デバイスの最初のホップ ルータ/スイッチ（MCU など）に CLI アクセスがあることを確認します。
- Mediatrace 統計については、次の点を確認します。
  - 接続元または接続先デバイスで 5 タプル（送信元アドレス、送信元ポート、宛先アドレス、宛先ポート、プロトコル）が使用可能です。
  - パスには Mediatrace イニシエータがあり、Mediatrace バージョンは 1.0 または 3.0 です（2.0 はサポートされていません）。
- MCU、CTMS、MXP、E20 などのデバイスでは、5 タプルは使用できません。

Cisco Prime Collaboration リリース 11.5 以前の場合

送信元	送信先
CTS	CTS、CTMS、C_CODEC、TPS、CIUS、MXP、IP フォン、Cisco Jabber、、E20、ルータ
C_CODEC	CTS、CTMS、VCS、C_CODEC、TPS、CIUS、MXP、IP フォン、Cisco Jabber、MCU、、E20、ルータ、
Cius	CTS、CTMS、C_CODEC、TPS、CIUS、MXP、IP フォン、Cisco Jabber、MCU、E20

送信元	送信先
MXP	CTS、CTMS、VCS、C_CODEC、TPS、CIUS、MXP、IP フォン、Cisco Jabber、MCUE20
電話	CTS、CTMS、VCS、C_CODEC、TPS、CIUS、MXP、IP フォン、Cisco Jabber、MCUE20
Cisco Jabber	CTS、CTMS、VCS、C_CODEC、TPS、CIUS、MXP、IP フォン、Cisco Jabber、MCUE20
POLYCOM	CTS、（CTMS）、VCS、C_CODEC、TPS、CIUS、MXP、MCU、IP フォン、Cisco Jabber、MCU、、E20
E 20	E20、CTS、（CTMS）、VCS、C_CODEC、TPS、CIUS、MXP、MCU、IP フォン、Cisco Jabber、MCU、
スイッチ	スイッチ、ルータ
ルータ	スイッチ、ルータ、C_CODEC、MCU、TPS、（CTMS）
VSAA	VSAA
CTMS	CTS、ルータ
MCU	C_CODEC、E20、MXP、CUIS、IP フォン、Cisco Jabber、、ルータ
TPS	C_CODEC、E20、MXP、CTS、CUIS、IP フォン、Cisco Jabber、、ルータ
VCS	C_CODEC、E20、MXP、CUIS、IP フォン、Cisco Jabber、

Cisco Prime Collaboration リリース 11.6 以降の場合

送信元	送信先
Cisco エンドポイント	Cisco エンドポイント、MCU、TP、仮想 TP、VG、CUBE、VCS、Expressway-Core、不明なエンドポイント

（注）
- Cisco Prime Collaboration Assurance は、ソース デバイスが 5 タプルの情報を含む Cisco エンドポイントである場合のみ、トラブルシューティングをサポートします。
- Cisco Prime Collaboration Assurance は、Cisco Jabber エンドポイントのトラブルシューティングはサポートしていません。

トラブルシューティング ワークフローの開始

[会議の診断（Conference Diagnostics）] ページの [360° 会議ビュー（360° Conference View）] から、会議のトラブルシューティング ワークフローを開始することができます。

Cisco Prime Collaboration リリース 11.1 以前の場合

（注） トラブルシューティングの時間を短縮するため、トラブルシューティングを開始する前には、メディア パスにあるデバイスを検出し、**[インベントリ（Inventory）]** で使用可能にしておくことを推奨します。

[エンドポイントの診断（Endpoint Diagnostics）] ページのクイック ビュー ウィンドウから、エンドポイントのトラブルシューティング ワークフローを開始できます。

Cisco Prime Collaboration リリース 11.6 以降の場合

表 *92 :* トラブルシューティング ワークフローの起動ポイント

トラブルシューティング タイプ	起動ポイント
自動	**1.** 選択 **[診断（Diagnose）]** > **[会議の診断（Conference Diagnostics）]**。 **2.** スケジュール済みの会議を選択します。 **3.** [ビデオ コラボレーション 会議（Video Collaboration Conference）] テーブルの [会議の件名（Conference Subject）] カラムにマウス ポインタを合わせ、[360° 会議（360° Conference）] ビュー アイコンをクリックします。 **4.** [Add to Watch List] をクリックします。

トラブルシューティング タイプ	起動ポイント
自動	**1.** 選択 **[診断（Diagnose）] > [会議の診断（Conference Diagnostics）]**。 **2.** [Not In Use] 使用ステータスになっているエンドポイントを選択します。 **3.** [List of Endpoints] テーブルの [Endpoint Name]列の上にマウスポインタを置いて、表示されるクイック ビュー アイコンをクリックします。 **4.** [Add to Watch List] をクリックします。 エンドポイントが会議に参加すると、トラブルシューティング ワークフローがすぐに開始します。
手動	**1.** 選択 **[診断（Diagnose）] > [会議の診断（Conference Diagnostics）]**。 **2.** 進行中の会議を選択します。アラームが設定された進行中の会議を選択することを推奨します。 **3.** [ビデオ コラボレーション 会議（Video Collaboration Conference）] テーブルの [会議の件名（Conference Subject）] カラムにマウス ポインタを合わせ、[360° 会議（360° Conference）] ビュー アイコンをクリックします。 **4.** アイコンをクリックして [Troubleshooting] ページを起動し、トラブルシューティングを開始する方向を選択します。

トラブルシューティング タイプ	起動ポイント
手動	1. 選択 **[診断（Diagnose）]** > **[会議の診断（Conference Diagnostics）]**。 2. [In Use] 使用ステータスになっているエンドポイントを選択します。 3. [List of Endpoints] テーブルの [Endpoint Name]列の上にマウス ポインタを置いて、クイック ビュー アイコンをクリックします。 4. [Add to Watch List] をクリックします。 トラブルシューティング ワークフローが即時に開始されます。

データ分析のトラブルシュート

会議またはエンドポイントで手動または自動のトラブルシューティングがアクティブな場合は、進行中の会議、ならびに完了した会議の両方で、トラブルシューティングデータを表示できます。

トラブルシューティング ジョブが完了すると、次のデータが表示されます。

トラブルシューティング

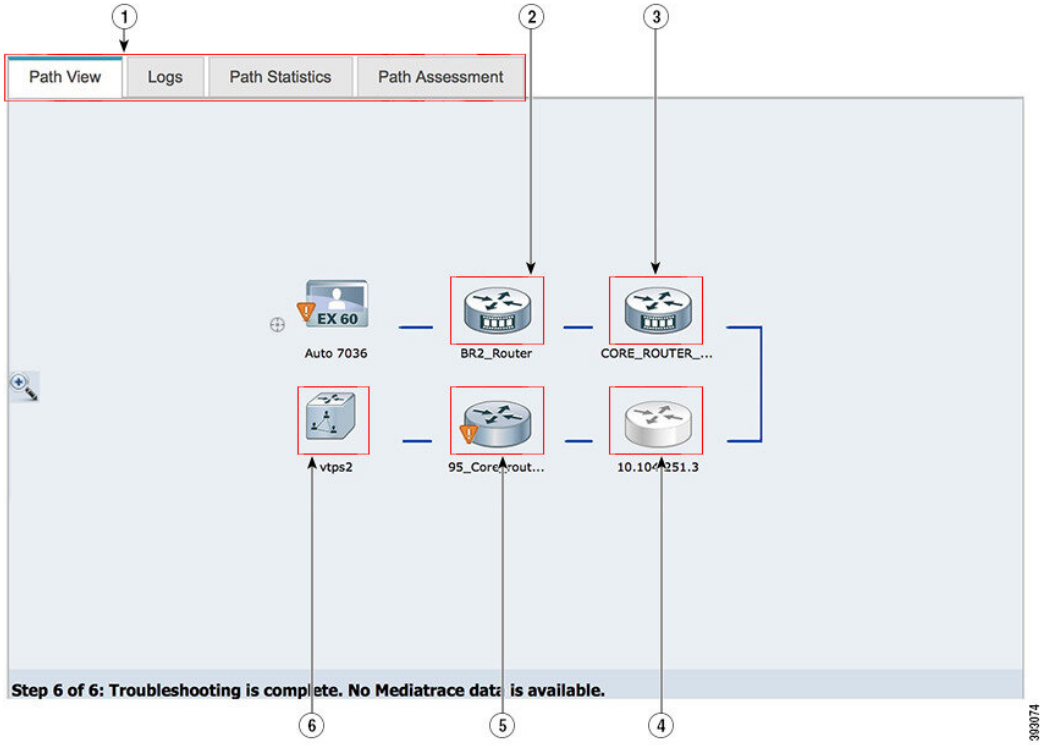
[パス ビュー（Path View）] タブでは、選択した方向のエンドポイント間のトポロジ（レイヤ 2 と 3）を表示できます。

- デバイス間を結ぶ線が直線の場合は、デバイスがお互いに直接接続されていることを示しており、。
- デバイス間を結ぶ線が点線の場合は、デバイスが接続されていない可能性があることを示しており、。

次の画像には、エンドポイント間にある会議のトラブルシューティングが示されています。

Cisco Prime Collaboration リリース 11.1 以前の場合

図 *11* : エンドポイント間のトラブルシューティング セッション

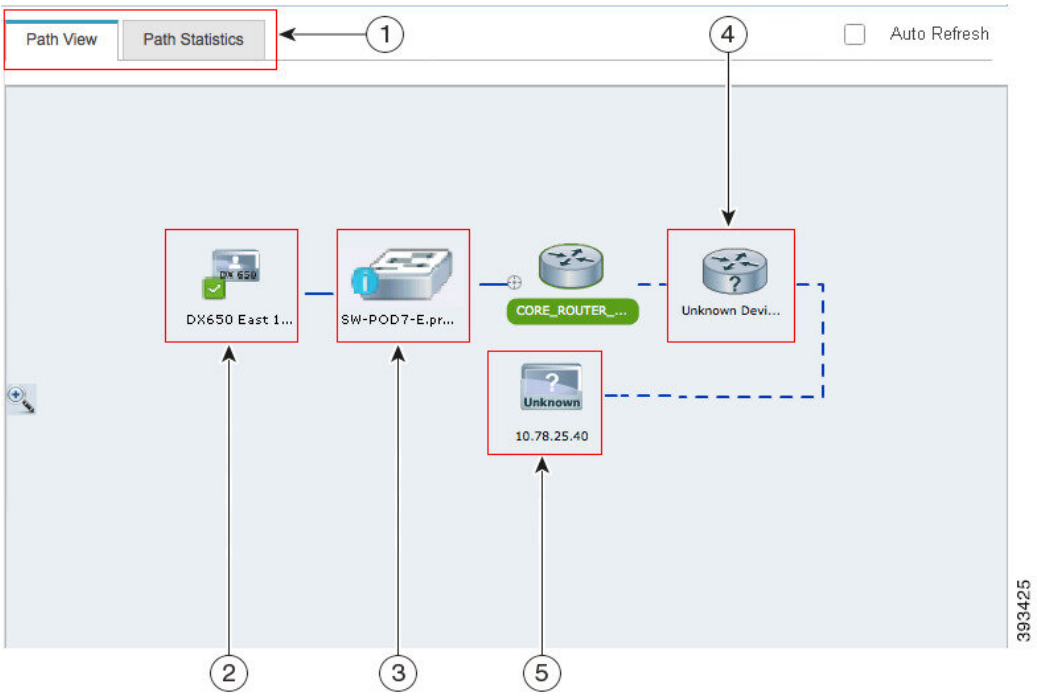


1	トラブルシューティング結果のタブです。 デバイスの設定（Mediatrace、Performance Monitor）によっては、一部のタブが表示されない場合があります。	2	Cisco Prime Network Analysis Module（Prime NAM）搭載のデバイスは、デバイス上に追加のバッジが付いて表示されます。アクセス不能なデバイスは、グレー表示になります。
3	Mediatrace がイネーブルになっているデバイスには、デバイス上に表示が追加されます。	4	アクセス不能なデバイスは、グレー表示になります。
5	エンドポイントに対するアラーム表示は、そのエンドポイントに障害があることを表します。	6	検出されたデバイス上の情報バッジは、メモリ、CPU使用率、またはコール品質統計（RTP パケット損失、RTP パケット ジッタ、DSCP）に問題があることを示しています。 コール品質統計と使用率(メモリと CPU)のしきい値は、[会議パスのしきい値の設定(Conference Path Threshold Settings) ページ **([アラームおよびレポート管理（Alarm & Report Administration）] > [会議パスのしきい値設定（Conference Path Threshold Settings）]**。

デバイスがアクセス可能な場合は、マウスポインタをそのデバイス上に置き、クイック ビューアイコンをクリックすることで、システムおよびインターフェイスの詳細を表示できます。

Cisco Prime Collaboration リリース 11.6 以降の場合

図 *12 :* エンドポイント間にある会議のトラブルシューティング



1	トラブルシューティング結果のタブです。	2	トラブルシューティングを開始した元のエンドポイントです。
3	パスにあるミッドポイント（ルータまたはスイッチ）です。中点にある青のバッジは、しきい値がすべてのデバイスの Rx パケット損失、ジッタ、または遅延で設定された制限値を超えたことを示します。 しきい値は、[会議パスのしきい値の設定 (Conference Path Threshold Settings] ページ) で定義します(**[アラームおよびレポート管理（Alarm & Report Administration）] > [会議パスのしきい値設定（Conference Path Threshold Settings）]**。	4	Cisco APIC-EM によって識別されない不明なデバイスです。不明なデバイスには疑問符（?）が付いて表示されます。
5	送信先エンドポイントです。 Cisco Prime Collaboration Assurance は、通知先デバイスまたはエンドポイントが [Unknown] な状態であったとしても、トラブルシューティングをサポートします。		

Cisco Prime Collaboration リリース 11.6 以降の場合

デフォルトでは、[会議のトラブルシューティング（Conference Troubleshooting）] ページは 30 秒ごとに自動更新されます。自動更新機能を無効にするには、[会議のトラブルシューティング（Conference Troubleshooting）] ページの右上隅にある **[自動更新（Auto Refresh）]** チェックボックスをオフにします。マウス ポインタをデバイスの上に置き、クイック ビュー アイコンをクリックすると、システム、インターフェイス、およびフローの詳細が表示されます。

次の表には、クイック ビューに一覧表示されるシステム、インターフェイス、フローの詳細が示されています。

Cisco Prime Collaboration リリース 11.1 以前の場合

表 *93* : システム、インターフェイス、およびフローの詳細

フィールド		説明
ホスト名		デバイスで設定されているホスト名です。
IP Address		デバイスを管理するために使用される IP アドレス。このリンクを使用して、エンドポイントまたはインフラストラクチャ デバイスのログイン ページを起動することができます。
Mediatrace Capable この情報は、デバイス上で Mediatrace が有効な場合のみに表示されます。	Mediatrace Role	デバイスに Cisco Mediatrace ロールを設定します。
	IP SLA Role	デバイスに IP SLA ロールを設定します。
	Performance Monitor	設定済みの Performance Monitor です。

フィールド		説明	
システム ステータス	Physical Memory Utilization (in%)	物理メモリ使用率（パーセンテージ）。	
	CPU Utilization (in%)	CPU 使用率（パーセンテージ）。	
	インターフェイスの詳細	Operation Status	インターフェイスの管理ステータス。ifOperStatus オブジェクトで指定。
Input Metrics		表示されるデータは RFC1213 MIB 属性に基づく。	
Output Metrics		表示されるデータは RFC1213 MIB 属性に基づく。	
ネットワーク診断	これは、これらのデバイスを Cisco Prime Network Analysis Module（Prime NAM）または Cisco Prime LMS で管理する場合のみ表示されます。		

フィールド		説明
メディア のフロー情報	次の情報はデバイスのすべての管理対象コーデックの統合レポートです。この情報は、デバイス上で Mediatrace が有効な場合のみに表示されます。	
	DSCP	デバイス上に設定された DSCP 値。
	IP パケット ドロップ数（IP Packet Drop Count）	ドロップされた IP パケットの数。
	RTP Packet Loss	リアルタイム転送プロトコル（RTP）が示すパケット損失。
	RTP Packet Jitter (RFC 3550)	リアルタイム転送プロトコル（RTP）が示すジッター。
	Ingress Interface	入力インターフェイスの詳細。
	Egress Interface	出力インターフェイスの詳細。

Cisco Prime Collaboration リリース 11.6 以降の場合

表 *94 :* システム、インターフェイス、およびフローの詳細

フィールド		説明
ホスト名		デバイスで設定されているホスト名です。
IP Address		デバイスを管理するために使用される IP アドレス。このリンクを使用して、エンドポイントまたはインフラストラクチャデバイスのログインページを起動することができます。
システム ステータス	Physical Memory Utilization (in%)	物理メモリ使用率（パーセンテージ）。
	CPU Utilization (in%)	CPU 使用率（パーセンテージ）。
インターフェイスの詳細	システム ステータス	インターフェイスの管理ステータス。ifOperStatus オブジェクトで指定。
	Input Metrics	表示されるデータは RFC1213 MIB 属性に基づく。
	Output Metrics	表示されるデータは RFC1213 MIB 属性に基づく。

フィールド		説明
メディア フロー情報 （注） –1 は、特定の統計データがプラットフォーム/デバイスから利用できないことを示します。		
	DSCP	デバイス上に設定された DSCP 値。
	IP パケット ドロップ数（IP Packet Drop Count）	ドロップされた IP パケットの数。
	RTP Packet Loss	リアルタイム転送プロトコル（RTP）が示すパケット損失。
	RTP Packet Jitter (RFC 3550)	リアルタイム転送プロトコル（RTP）が示すジッター。
	Ingress Interface	入力インターフェイスの詳細。
	Egress Interface	出力インターフェイスの詳細。

パス統計

パス統計ビューには、パス内の各ノードの統計情報が表示されます。

次のグラフには、パス統計ビューが表示されています。

CPU および メモリ

グラフにはすべてのデバイスが表示され、次の情報が含まれています。

- 縦軸（y 軸）は、過去 5 分間の CPU 使用率の詳細をパーセンテージで表します。
- 横軸（X 軸）にはパス トレースで検出されたネットワーク デバイスすべてがリストされます。
- グラフ内の球体は、プロセッサ メモリ使用率の詳細をパーセンテージで表します。球体のツール チップには、メモリ使用率の正確な値が表示されます。
- 球体の大きさは、プロセッサ メモリ使用率によって変化します。球体のサイズが小さい場合、プロセッサ メモリ使用率が低いことを示します。

球体（赤いアイコン）をクリックすると、システム、インターフェイス、フローの詳細が表示されます。

CPU and Packet Loss

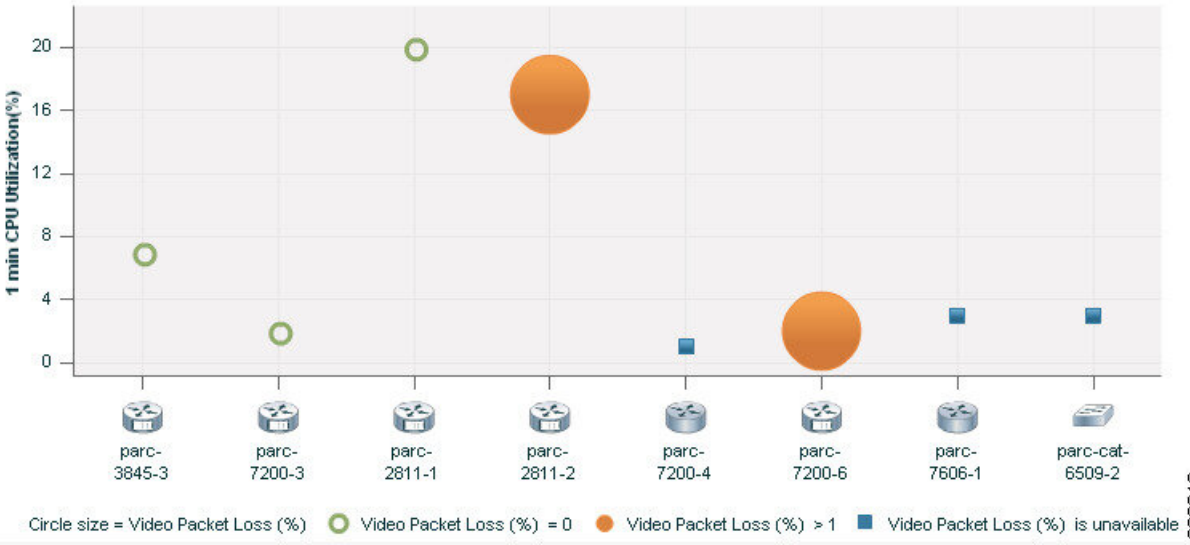
このグラフは、すべてのデバイスに表示され、次の情報を含んでいます。

- 縦軸（y 軸）は、過去 5 分間の CPU 使用率の詳細をパーセンテージで表します。

- 横軸（X 軸）にはパス トレースで検出されたネットワーク デバイスすべてがリストされます。
- グラフ内の球体は、ビデオ パケット損失の詳細をパーセンテージで表します。
  - グリーンの球体は、ビデオ パケット損失がゼロであることを示します。
  - オレンジの球体は、ビデオ パケット損失が 1 % を超えることを示します。球体の大きさは、ビデオパケット損失によって変化します。球体のサイズが小さい場合、ビデオ パケット損失が少ないことを示します。

    球体をクリックすると、インターフェイス レベルでのパケット損失をより詳細に分析できます。
  - 青い正方形のボックスは、perfmon カウンタの統計情報がデバイスから利用できないことを示します。

図 *13 : CPU and Packet Loss* グラフ



球体または正方形のボックス（赤いアイコン）をクリックすると、システム、インターフェイス、および フローの詳細が表示されます。

Video IP Bit Rate and Packet Loss

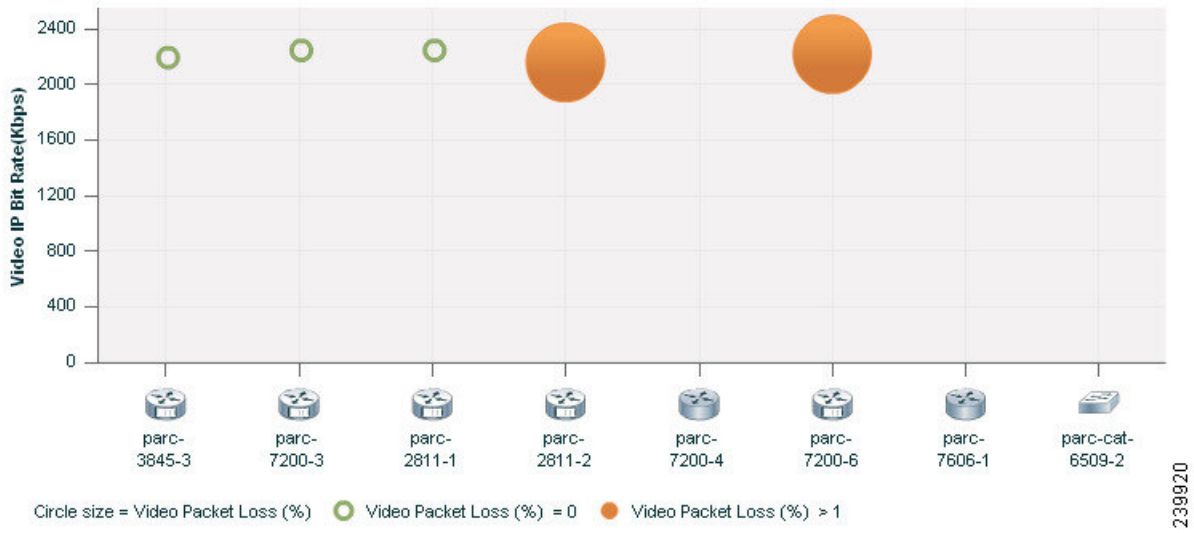
このグラフは、すべてのデバイスに表示され、次の情報を含んでいます。

- 縦軸（Y 軸）には、ビデオ IP ビット レートがキロビット毎秒（kbps）で表示されます。
- 横軸（X 軸）にはパス トレースで検出されたネットワーク デバイスすべてがリストされます。
- グラフ内の球体は、ビデオ パケット損失の詳細をパーセンテージで表します。
  - グリーンの球体は、ビデオ パケット損失がゼロであることを示します。

- オレンジの球体は、ビデオ パケット損失が 1 % を超えることを示します。球体の大きさは、ビデオパケット損失によって変化します。球体のサイズが小さい場合、ビデオ パケット損失が少ないことを示します。

  球体をクリックすると、インターフェイス レベルでのパケット損失をより詳細に分析できます。

図 *14 : Video IP Bit Rate and Packet Loss* グラフ



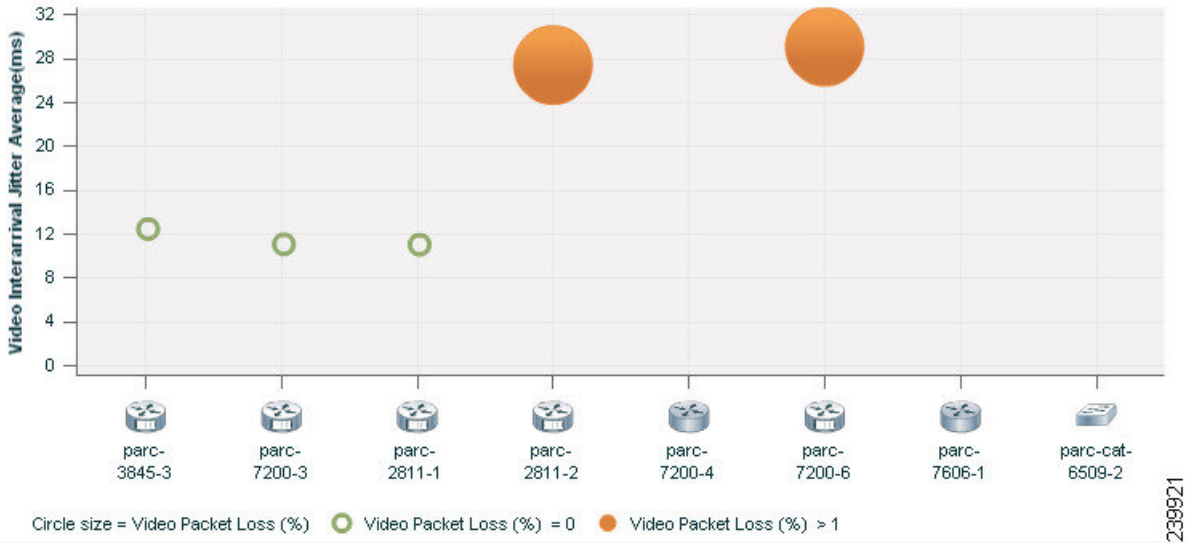
球体（赤いアイコン）をクリックすると、システム、インターフェイス、フローの詳細が表示されます。

Video Interarrival Jitter and Packet Loss

このグラフは、すべてのデバイスに表示され、次の情報を含んでいます。

- 縦軸（Y 軸）は平均ビデオ到着時間間隔ジッター値を示します（ミリ秒単位）。
- 横軸（X 軸）にはパス トレースで検出されたネットワーク デバイスすべてがリストされます。
- グラフ内の球体は、ビデオ パケット損失の詳細をパーセンテージで表します。
  - グリーンの球体は、ビデオ パケット損失がゼロであることを示します。
  - オレンジの球体は、ビデオ パケット損失が 1 % を超えることを示します。球体の大きさは、ビデオパケット損失によって変化します。球体のサイズが小さい場合、ビデオ パケット損失が少ないことを示します。

図 *15 : Video Interarrival Jitter and Packet Loss* グラフ



球体（赤いアイコン）をクリックすると、システム、インターフェイス、フローの詳細が表示されます。

IP DSCP およびパケット損失

このグラフは、すべてのデバイスに表示され、次の情報を含んでいます。

- 縦軸（Y 軸）は、平均 IP DiffServ コード ポイント（DSCP）を示します。この値は、デバイスで事前に設定されています。
- 横軸（X 軸）にはパス トレースで検出されたネットワーク デバイスすべてがリストされます。
- グラフ内の球体は、ビデオ パケット損失の詳細をパーセンテージで表します。
  - グリーンの球体は、ビデオ パケット損失がゼロであることを示します。
  - オレンジの球体は、ビデオ パケット損失が 1 % を超えることを示します。球体の大きさは、ビデオパケット損失によって変化します。球体のサイズが小さい場合、ビデオ パケット損失が少ないことを示します。

球体（赤いアイコン）をクリックすると、システム、インターフェイス、フローの詳細が表示されます。

トラブルシューティング データのエクスポート

データをエクスポートできるのは、会議が終了した後のみです。トラブルシューティング ジョブが完了すると、[会議モニタリング（Conference Monitoring）] ページにトラブルシューティング ジョブのステータスが表示されます。

トラブルシューティング データをエクスポートするには、次の手順を実行します。

ステップ 1 選択 **[診断（Diagnose）] > [セッションの診断（Session Diagnostics）]**。

[セッション診断（Session Diagnostics ）] ページが表示されます。

Cisco Prime Collaboration リリース 11.5 以降の場合

選択 **[診断（Diagnose）] > [会議の診断（Conference Diagnostics）]**。

[会議の診断（Conference Diagnostics）] ページが表示されます。

ステップ 2 トラブルシューティング ステータスのアイコンに「トラブルシューティング レポートが利用可能（Troubleshooting Report Available）」と表示される、過去の[会議（conference）] を選択します。

ステップ 3 [ビデオコラボレーション会議（Video Collaboration Conference）] テーブルの [会議の件名（Conference Subject）] 列にマウス ポインターを合わせ、[360°会議（360° Conference）] ビュー アイコンをクリックします。

ステップ 4 [360°会議（360° SessionConference）] ビュー ウィンドウの [トラブルシューティングデータのエクスポート（Export Troubleshooting Data）] アイコンをクリックします。

HTML ファイル形式のトラブルシューティング レポートが新しいブラウザ ウィンドウに表示されます。

トラブルシューティング レポートのエクスポートを理解する

トラブルシューティング レポートをエクスポートすると、次の詳細情報が含まれます。

レポートのフィールド	説明
Conference Identifier	会議用の一意な ID です。
Conference Subject	会議がアドホック、スケジュール済み、またはスタティックかを表示します。
Conference Date	会議が行われた日付です。
Conference Start Time	会議の開始時間です。
Conference Duration in Minutes	会議の長さです。
Conference Type	会議がポイント ツー ポイントか、またはマルチポイントかを表示します。
Endpoints	会議の一部であったエンドポイントの詳細です。
Call Segment	トラブルシューティング中に使用された方向を表示します。

レポートのフィールド	説明
Troubleshooting Conference	トラブルシューティング ワークフローの開始時刻と終了時刻。
Troubleshooting Conference ID	トラブルシューティング ワークフローの固有ID。
Troubleshooting Start Time	トラブルシューティング ワークフローの開始時刻です。
Troubleshooting Initiation	トラブルシューティングが手動で開始されたか、自動的に開始したかを表示します。
Path Topology and Metrics	トラブルシューティングパストポロジとメトリクスについての情報を表示します。 フィールドとその説明は、次のとおりです。 • ホスト名/IPアドレス：ホスト名またはIPアドレスです。 • [CPU Utilization (Max, Avg)]：CPU 使用率の最大と平均を表示します。 • [Memory Utilization (Max, Avg)]：メモリ使用率の最大と平均を表示します。 • [Packet Loss (Video, Audio)]：ビデオおよびオーディオの最大パケット損失を表示します。 • [Max Jitter (Video, Audio)]：ビデオとオーディオの最大ジッターを表示します。 • [DSCP (Video, Audio)]：ビデオおよびオーディオの DSCP 値を表示します。
Troubleshooting End Time	トラブルシューティング ワークフローの開始時刻。
Troubleshooting Termination	トラブルシューティング ワークフローが手動で終了されたか、自動的に停止したかを表示します。

Cisco Prime Infrastructure のクロス起動

Cisco Prime Collaboration Assurance では、Infrastructure アプリケーションを使用してネットワーク診断を実行できます。Cisco Prime Collaboration Assurance では、Cisco Prime Infrastructure バージョン 4.1 および 4.2 がサポートされています。

Cisco Prime Collaboration Assurance で Cisco Prime Infrastructure を起動するには、Cisco Prime Infrastructure のホスト名とユーザ クレデンシャルが必要です。

前提条件：

- デバイスが Cisco Prime Infrastructure と Cisco Prime Collaboration Assurance アプリケーションの両方で管理されていることを確認する必要があります。
- ルータおよびスイッチに必要なすべてのクレデンシャルが Cisco Prime Collaboration Assurance に追加されていることを確認する必要があります。詳細については、『Cisco Prime Collaboration Assurance 用デバイスのセットアップ』を参照してください。
- Cisco Prime Infrastructure ソフトウェアのあるネットワーク デバイスが Cisco Prime Collaboration Assurance からアクセス可能であることを確認する必要があります。

Cisco Prime Infrastructure のユーザ権限に基づいて、Cisco Prime Infrastructure アプリケーションの次の機能を起動することができます。

- [デバイスビュー（Device View）]：ネットワーク デバイスのリアルタイム ビューを提供するグラフィカルなデバイス管理ツールです。これらのビューは、定期的に更新される、デバイス構成とパフォーマンス条件の物理的な画像を提供します。
- [接続されたホスト（Connected Hosts）]：アクセス スイッチに接続されているすべてのホストの詳細を表示します。
- [変更監査レポート（24時間）（Change Audit Report (24 hours)）]：過去 24 時間にデバイスで発生したすべての変更の概要を表示します。ソフトウェアイメージ、コンフィギュレーション ファイル、およびハードウェアに対する変更点が含まれます。
- [設定の表示/編集（View/Edit Configuration）]：アーカイブされているデバイスの設定ファイルを、未加工の状態および処理された形式で表示します。必要な権限がある場合は、コンフィギュレーション ファイルを編集することもできます。
- [障害（24時間）（Faults (24 hours)）]：過去 24 時間にデバイスでトリガーされたアラートとイベントの詳細を表示します。
- [Syslogメッセージ（Syslog Messages）]：デバイスでトリガーされた syslog メッセージの詳細を表示します。
- [システムパフォーマンス（System Performance）]：メモリ使用率、CPU 使用率、インターフェイス使用率、周辺温度、ポーリングの失敗など、デバイスのパフォーマンスパラメータをすべて表示します。

Cisco Prime Infrastructure のクロス起動

（注） **Cisco Prime Collaboration リリース 11.5 以降の場合**

[360 Integration] ページからの Cisco Prime Infrastructure のクロス起動は、Cisco Prime Collaboration Assurance 11.5 ではサポートされていません。

CCisco Prime Infrastructure のクロス起動を設定するには、次の手順を実行します。

ステップ 1 選択 **[システム管理（System Administration）]** > **[360の統合（360 Integration）]**。

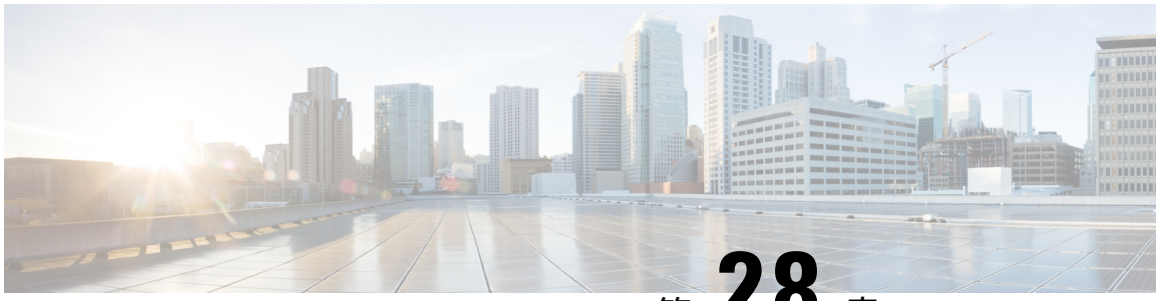
ステップ 2 [Cisco Prime Infrastructure セットアップ （Cisco Prime LMS Infrastructure Setup）] ペインに、必要な詳細を入力します。フィールドの説明の詳細 については、「Cisco Prime Infrastructure ペイン：フィールドの説明」を参照してください。

ステップ 3 [保存（Save）] をクリックします。

Cisco Prime Infrastructure ペイン：フィールドの説明

表 *95 : Cisco Prime Infrastructure* ペインのフィールドの説明

フィールド	説明
Cisco Prime Infrastructure サーバ	Infrastructure サーバのホスト名または IP アドレス。 Cisco Prime Infrastructureをマルチサーバ セットアップで展開した場合は、Cisco Prime Infrastructure のマスター サーバの詳細を入力する必要があります。
Prime Infrastructure のユーザとパスワード	Cisco Prime Infrastructure サーバに設定されているダミー ユーザ。 Cisco Prime CM サーバは、これらのクレデンシャルを使用して、Cisco Prime Infrastructure サーバと内部的にやり取りします。このユーザには、Cisco Prime Infrastructure サーバに対する管理関連の権限を割り当てないでください。



第 28 章

メディア パスの分析

このセクションでは、次の点について説明します。

- メディア パスの分析 （681 ページ）

メディア パスの分析

この章では、メディア パスの分析のさまざまな分析方法について説明します。

VSAA を使用したメディア パスの分析

Video SLA Assessment Agent（VSAA）は、Cisco Prime Collaboration Assurance で、Cisco Video、テレプレゼンス、またはIP ビデオ監視（IPVS）システムとサイトの拡張機能を導入またはアップグレードする前に、ネットワーク パス特性（つまり、遅延、ジッタ、パケット ロス）を提供するために使用されます。

始める前に

（注） Cisco Prime Collaboration Assurance を MSP モードで導入した場合、メディア パス分析は NAT 環境ではサポートされません。

VSA エージェントが 2 つのエンドポイントで動作中であり、NTP サーバに同期されていることを確認します。VSA エージェント ソフトウェアを、Cisco.com にある Cisco Prime Collaboration Assurance ソフトウェア ダウンロード サイトからダウンロードすることができます。インストール ガイドラインについては、「Video SLA Assessment Agent 3.1 インストール ガイド」を参照してください。

ステップ 1 選択 **[診断（Diagnose）] > [Media Path Analyzer]**。

ステップ 2 必要なアセスメントの詳細を入力します。

ステップ 3 表 96 : プロファイルの詳細を入力します。

ステップ 4 [Start] をクリックします。

表 *96 :* プロファイルの詳細

フィールド	説明
Profile	検査するプロファイル設定を表示します。送信される RTP パケットは、デバイス タイプに基づいたものになります。
Count	ネットワークに追加するデバイスまたはストリームの数。最大 5 個のデバイスを追加できます。
DSCP	DSCP 値は、トラフィック品質のプライオリティを示します。良質のビデオ ストリーミングを確保できるよう、最も高品質の DSCP 値が選択されます。

CTS 500 と 1000 を導入するには CTS1000 プロファイルを使用し、CTS 3000 を導入するには CTS3000 プロファイルを使用する必要があります。プロファイルを作成、編集、および削除できます。

VSA エージェントの検査結果

個々のストリームについて、エンドポイント間で選択した方向のトポロジ（レイヤ 2 とレイヤ 3）を [トラブルシューティング（Troubleshooting）] タブで表示できます。

[ログ（Log）] タブを使用して、上位レベルおよび個別ストリームに対するトラブルシューティング ワークフローのステータスを詳しく表示することができます。。[VSA エージェントの検査結果（VSA Agent Assessment Result）] では、[パス評価（Path Assessment）] タブでパスの詳細を確認することもできます。テスト可能デバイス、テスト不可能デバイス、パケット損失のしきい値に違反するデバイス、ジッターのしきい値に違反するデバイス、DSCP に違反するデバイスで、トラブルシューティングの概要情報を表示できます。

トラブルシューティングで判別されたデバイスに対して、一連のテストが実行されます。Path Assessment テストを開始するには、および会議のプロアクティブなトラブルシューティングが完了した後に、[Path Assessmentテスト（Path Assessment Tests）] をクリックします。

[テスト結果（Test Result）] タブには、次のグラフが表示されます。これらのチャートには、最後の 20 件のテスト結果のみが表示されます。

テストの要約

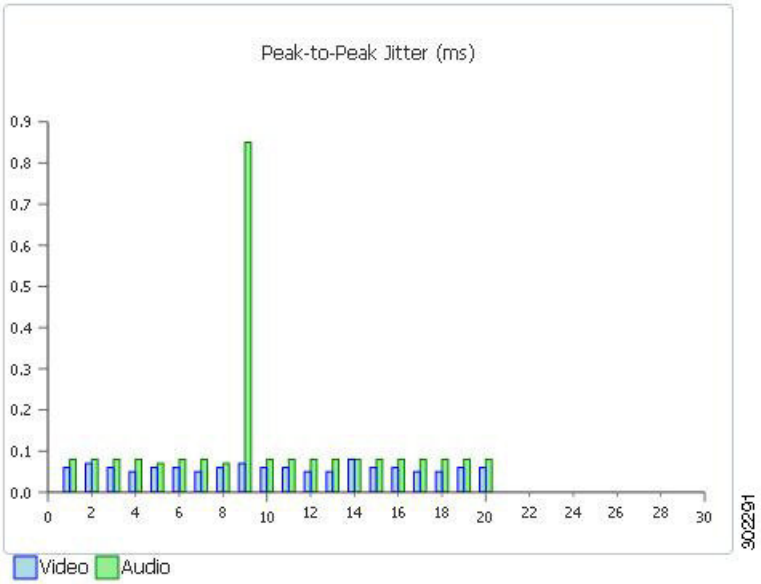
図 *16 :* テストの要約

Statistics	Video Result	Audio Result
DSCP	af42(36)	af42(36)
Profile	CTS-1000	CTS-1000
Max Rate	30.02 frames/s	50.04 packets/s
Total Packets Recieved	439079 packets	44627 packets
Total Packet loss due to Network Drops	0 packets	0 packets
Maximum Seconds of Concealment	0.0 s	0.0 s
Maximum Severe Seconds of Concealment	0.0 s	0.0 s
Maximum Packet Loss	0.0 %	0.0 %
Maximum Jitter	0.01 ms	0.03 ms
Maximum Peak-to-Peak jitter	0.81 ms	0.85 ms
Maximum Peak Playout Delay	0.87 ms	0.83 ms
Maximum Latency	2.32 ms	2.31 ms
Maximum Frame Jitter Average	0.01 ms	0.0 ms
Time Obtained	2012-May-03 21:47:52 PDT	2012-May-03 21:47:52 PDT

302292

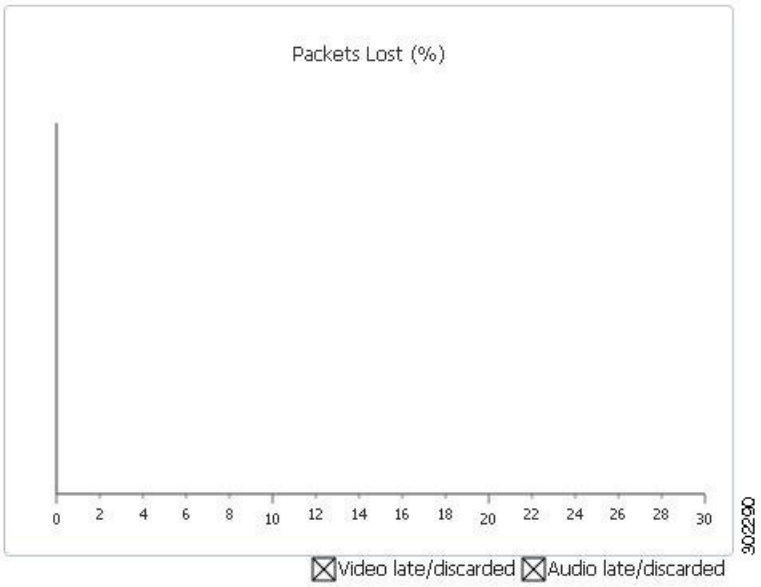
ピークツーピーク ジッター

図 *17 :* ピークツーピーク ジッター グラフ



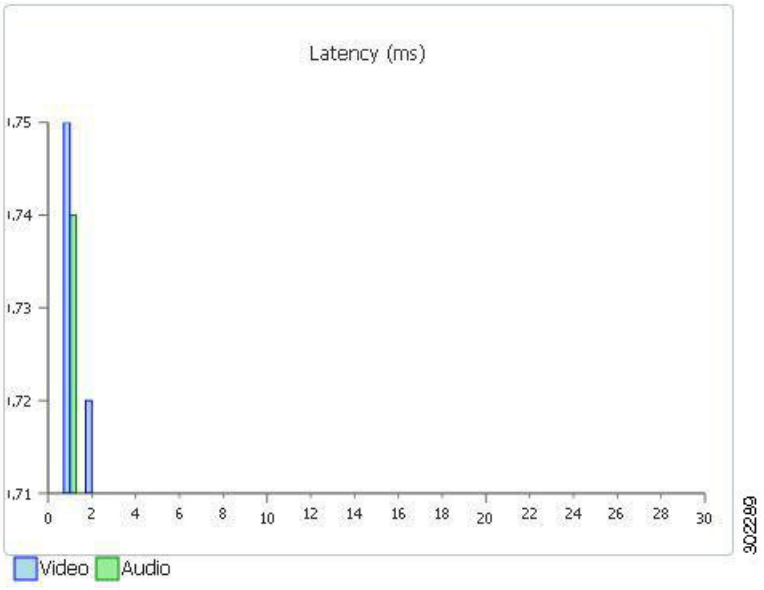
パケット ロス（Packets Lost）

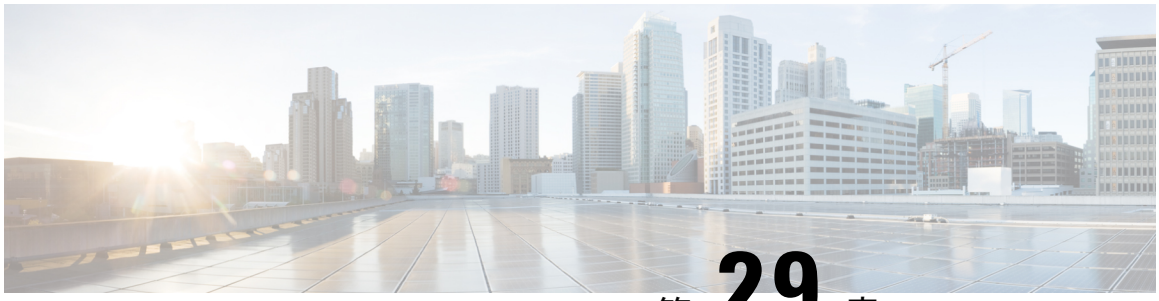
図 *18 :* パケット ロス グラフ



遅延

図 *19 :* 遅延グラフ





第 29 章

ログの収集

このセクションでは、次の点について説明します。

- ログの収集 （685 ページ）
- ログ収集センター/デバイス ログ コレクター （686 ページ）
- トレース レベルの設定 （689 ページ）
- ログ収集テンプレート （690 ページ）
- コール ログの収集 （690 ページ）

ログの収集

Cisco Prime Collaboration Assurance を使用すると、コール ログを収集して、Cisco Voice Portal（CVP）、Unified Contact Center Enterprise（Unified CCE）、Cisco Unified Communications Manager（Unified CM）、Cisco Unity Connection（CUC）、Cisco IM and Presence（Cisco IM & P）、Cisco IOS ゲートウェイでの障害を識別できます。この機能により、コールの問題のトラブルシューティングができます。SIP Call Flow Analyzer 機能を使用し、収集したコールをさらに詳しく調べて、メッセージ内の問題点を特定することができます。また、問題の再現にも役立ちます。SIP Call Flow Analyzer 機能の詳細については、「コール シグナリングの分析」を参照してください。

具体的には、次のような点で役立ちます。

- コールの問題のトラブルシューティングのためのコストを削減する。
- コールの問題のトラブルシューティングのための時間を短縮する。

前提条件

- Cisco Prime Collaboration Assurance のユーザ インターフェイスを使用して、デバイスのデバッグ レベルを設定します。

この機能の要件およびサポートされる内容は次のとおりです。

この機能に必要な最大ディスク サイズ。	小規模のプロファイル場合は 25 GB、中規模および大規模のプロファイルの場合は 50 GB。

同時にログ収集対象にできるデバイスの最大数。	100
同時に実行されるログ収集ジョブの最大数	3
1つのインスタンスでダウンロードできる zip 形式のログ ファイルの最大サイズ。	小規模のプロファイルの場合は 0.5 GB、その他のプロファイルの場合は 1 GB。 （注） このサイズには、すべてのデバイスとコールが含まれています。zip ファイルのサイズが上記のサイズを超えると、ログは複数の zip ファイルに分割されます。小規模のプロファイルの場合は 0.5 GB のファイルに、その他のプロファイルの場合は 1 GB のファイルに分割されます。

（注）
- System CLI ツール、または別の Cisco Prime Collaboration Assurance サーバ 10.5 以降から収集したログのみがサポートされています。
- デバイスのタイム ゾーンは System CLI ツールからは収集されません。
- この機能では、デバイスインベントリ にないデバイスのログも提供します。
- オペレータおよびヘルプデスク ユーザはデバイスからコール ログを収集できません。また、**[デバイス ログ コレクタ（Device Log Collector）]** メニュー ページへアクセスすることもできません。

ログ収集センター/デバイス ログ コレクター

Cisco Prime Collaboration リリース 11.5 以降の場合

Cisco Prime Collaboration Assurance を使用すると、次のページで使用できるデバイス ログ コレクタから通話ログを収集できます。 **[診断（Diagnose）]** > **[デバイス ログ コレクター（Device Log Collector）]** 次の Unified Communications(UC)コンポーネントの場合は、次のようになります。

デバイス タイプ	サポートされるリリース	コンポーネントまたはログのタイプ
Cisco Unified Communications Manager（Unified CM）	9.x 以降	すべての
IOS ゲートウェイ（TDM、CUBE（Enterprise Edition）、VXML GW）	15.1(4)M 以降	show logging コマンドの出力
Cisco Unity Connection（CUC）	9.x 以降	すべて

デバイス タイプ	サポートされるリリース	コンポーネントまたはログのタイプ
Cisco IM and Presence	9.x 以降	すべて

[Devices] ペイン

[Devices] ペインでは次の情報を使用できます。

- [Hostname]：デバイスのホスト名
- [IP Address]：デバイスの IP アドレス
- デバイス タイプ
- のデバイス インベントリで管理 - デバイスがのデバイス インベントリ で管理状態にあるかどうかを表示します。コラム値が [いいえ（No）] の場合、デバイスはのデバイス インベントリにはなく、のデバイス ログ コレクタのみに追加されているか、デバイスはのデバイス インベントリで Managed 状態にはないことを示します。
- 接続ステータス - デバイスは、のデバイス ログ コレクタで提供されているクレデンシャルを使用してアクセスできるかどうかを表示します。
- [TimeZone]：デバイスのタイム ゾーンを表示します。

のデバイス インベントリにあるデバイス（UC コンポーネント）をのデバイス ログ コレクタに追加または更新するには、デバイスを選択するか、すべてのデバイス グループを選択し、**の [インベントリ管理に同期（Sync to Inventory Management）]** をクリックします。のデバイス ログ コレクタおよび の**デバイス インベントリ**にあるデバイスは、次の方法で同期されます。

- 自動： のデバイス インベントリにあるデバイスは、1 時間ごとに同期されます。
- 手動：の **[インベントリ管理に同期（Sync to Inventory Management）]** ボタンをクリックすると、 のデバイス インベントリにある UC コンポーネントは、のデバイス ログ コレクタにあるデバイス リストに追加されます。

定期的な同期は1時間ごとに実行されます。のデバイスインベントリ内のデバイスが削除されている場合、同期したとしても のデバイス ログ コレクタからデバイスは削除されません。新しいデバイスがのデバイスログコレクタに追加またはデバイスが更新された場合、接続ステータスは同期後に更新されます。

（注）
- 同期は、 のデバイス インベントリからのデバイス ログ コレクタのみへと行われます。
- 同期後に、 のデバイスログコレクタのクレデンシャルは、 のデバイスインベントリのクレデンシャルによって上書きされます。したがって、デバイス インベントリと デバイス ログ コレクタでは、同じクレデンシャルの使用を推奨します。
- のデバイス インベントリでは、Managed 状態にあるデバイスのみが同期されます。
- DWC デバイス インベントリ<内のデバイスが削除され、 のデバイス ログ コレクタ内では削除されていない場合でも、のデバイス ログ コレクタではログ収集を実行できます。
- DWC デバイス インベントリ IOS ゲートウェイに CLI クレデンシャルがない場合、のデバイス ログ コレクタには同期されません。

デバイスのグループ化

同じ時間に同じタイプの UC コンポーネントからログを収集するには、UC コンポーネントのカスタム グループを作成して、デバイス グループを選択してコールを収集します。

事前定義されているグループを追加、編集、削除することも、グループ内のデバイスを変更することもできません。

ユーザ定義のグループを作成、編集、または削除することができます。ユーザ定義のグループのデバイスは追加、または削除することができます。次を実行できます。

Cisco Prime Collaboration リリース 11.5 以降の場合

タスク	詳細
グループの作成	をクリックします。**[診断（Diagnose）] > [デバイス ログ コレクタ（Device Log Collector）] > [グループ（Group）] > [新規作成（Create New）]**。
グループの編集	をクリックします。**[診断（Diagnose）]>[デバイス ログ コレクター（Device Log Collector）]**の順にクリックしてデバイスまたはグループを選択し、**[グループ（Group）] > [グループの編集（Edit Group）]**をクリックします。
グループの削除	をクリックします。**[診断（Diagnose）]>[デバイス ログ コレクター（Device Log Collector）]**の順にクリックしてデバイスまたはグループを選択し、**[グループ（Group）] > [グループの削除（Delete Group）]**をクリックします。所要時間
グループへのデバイスの追加	をクリックします。**[診断（Diagnose）]>[デバイス ログ コレクター（Device Log Collector）]**の順にクリックしてデバイスまたはグループを選択し、**[グループ（Group）] & [グループの削除（Delete Group）]**をクリックします。所要時間
グループからのデバイスの削除	をクリックします。**[診断（Diagnose）]>[デバイス ログ コレクター（Device Log Collector）]**でデバイスを選択し、**[グループ（Group）] > [グループに追加（Add to Group）]** をクリックします。
グループ内のデバイスの表示	Device Group Center からグループを選択します。グループのデバイスが [Devices] ペインに表示されます。

その他のタスク

次のタスクは、の [デバイス ログ コレクタ（Device Log Collector）] ページのデバイス ペインから実行できます。[Devices]ペインからタスクの実行対象にするデバイスを選択し、必要に応じて次の処理を実行します。

タスク	詳細
クレデンシャルの変更	デバイスのポート番号またはクレデンシャルの詳細を変更するには、**[クレデンシャルの変更（Modify Credentials）]** ボタンをクリックします。デバイス タイプは変更できません。

タスク	詳細
タイム ゾーンの変更	デバイスのタイム ゾーンを変更するには、**[タイム ゾーンの変更（Modify Time Zone）]** ボタンをクリックします。デフォルトでは Cisco Prime Collaboration Assurance サーバのタイム ゾーンが表示されます。

デバイスの接続テスト

指定されたクレデンシャルでデバイスにアクセスできるかどうかをテストするには、デバイスを選択して **[接続性テスト（Test Connectivity）]** ボタンをクリックします。メッセージが表示され、結果がユーザに通知されます。「[接続ステータス（Connectivity Status）」列の値は、必要に応じて更新されます。

接続テストのトラブルシューティング

接続テストに失敗した場合は、次の内容を確認してください。

- ポート番号。
- デバイスのクレデンシャル情報が、のデバイスインベントリのものと同じであることを確認します。
- Cisco Prime Collaboration Assurance Server からデバイスへの ping が正常であること。

トレース レベルの設定

この機能は、デバイスの各コンポーネントに対してトレース レベルを設定する場合に便利です。次のデバイスに対してトレース レベルを設定できます。

- Cisco Unified Communications Manager
- IOS ゲートウェイ
- Customer Voice Portal
- Cisco Unity Connection
- Cisco IM and Presence

Cisco Prime Collaboration リリース 11.5 以降の場合

移行方法 **[診断（Diagnose）]** > **[デバイス ログ コレクター（Device Log Collector）]**。

トレース レベルを設定する 1 つ以上のデバイスを選択して **[Set Trace Level to Devices]** ボタンをクリックします。[Set Trace Level to Devices] ポップアップ ウィンドウが表示されます。[デバイス タイプ（Device Type）] ドロップダウン リストからデバイスを選択します。選択したデバイスのコンポーネントがリストされます。発生した問題に関連するコンポーネントについて、適切なトレース レベル（[No Change]、[Default]、[Warning]、[Information]、[Debug]）を選択して [Apply] ボタンをクリックします。

（注） トレース レベルの設定により、ネットワークのパフォーマンスが低下することがあります。

ログ収集テンプレート

ログ収集テンプレートを使用して、複数のデバイスとコンポーネントのログをまとめて収集することができます。ログを収集するには、テンプレートの使用が必要です。新しいテンプレートを作成することも、デフォルトのテンプレートを使用することもできます。

テンプレートを作成するには、次の手順を実行します。

ステップ 1 **Cisco Prime Collaboration リリース 11.5 以降の場合**

選択 **[診断（Diagnose）]** > **[デバイス ログ コレクター（Device Log Collector）][トレーステンプレートの管理（Manage Trace Template）]** ボタンをクリックします。

ステップ 2 [Manage Trace Template] ペインで [Add] をクリックします。

ステップ 3 テンプレート名と説明を入力し、[Component] ペインでデバイス タイプとコンポーネントを選択します。複数（またはすべて）のデバイスとコンポーネントを選択することもできます。コンポーネントの詳細については、の「ログ収集センター/デバイス ログ コレクター」を参照してください。

使用できるデフォルトのテンプレート（コール トレースと呼ばれる）があります。このテンプレートには 4 つのデバイス タイプ（Unified CM、Unified CCE、CVP、IOS ゲートウェイ）があり、あらかじめ選択されているコンポーネントがあります。このテンプレートは変更できません。

ステップ 4 **[Save（保存）]** をクリックします。テンプレートが正常に保存されたことを通知するメッセージが表示されます。[Manage Trace Template] ページの [Templates] の下に新しいテンプレートが表示されているのが確認できます。

特定のテンプレートのコンポーネントを表示するには、テンプレートを選択して [Summary] をクリックします。テンプレートを変更するには、テンプレートを選択します。テンプレート名、説明、およびコンポーネントを変更できます。テンプレートを削除するには、テンプレートを選択して [Delete] をクリックします。

（注） テンプレートを作成、編集、および削除できるのはスーパー管理者のみです。他のユーザは、テンプレートの概要を表示することと、ログの収集用にテンプレートを使用することだけが可能です。

コール ログの収集

ログの収集はオンデマンドで実行されます。

グループ内の 1 つ以上のデバイスを選択し、[Collect Logs] ボタンをクリックしてログを収集します。[Collect Logs] ダイアログボックスが表示されます。必要な情報を入力します。ジョブ名とファイル名は自動的に入力されますが、修正することもできます。ここで選択したタイムゾーンがログの収集に使用されます。

[Use Template] ドロップダウン リストからテンプレートを選択します。

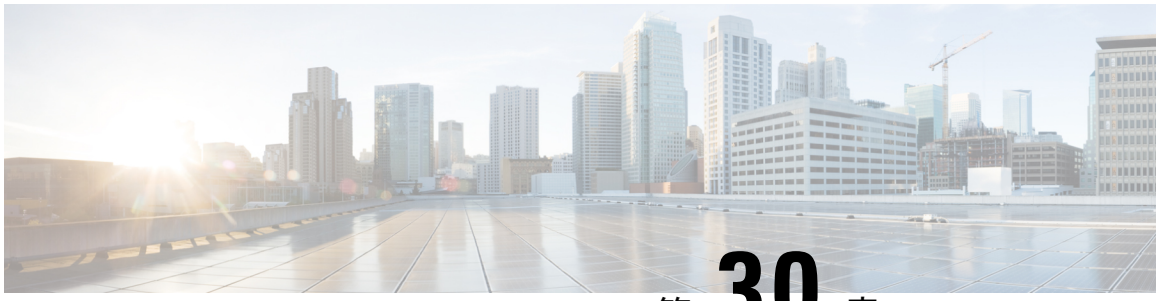
[Run] をクリックします。ジョブがトリガーされるかどうかを通知するメッセージが表示されます。ジョブは、[Log Collection Jobs] ペインの下に一覧表示されます。[Progress Status] 列には、ログの収集対象として選択されたデバイスの総数の中で、ログがダウンロードされたデバイスの数が示されます。たとえば、2 of 3（3 台のうち 2 台）となります。[Download to local] ボタンをクリックすると、ジョブを選択してログを収集できます。zip で圧縮されたファイルサイズが（小規模のプロファイルで）0.5 GB を超えている場合、または（中規模または大規模のプロファイルで）1 GB を超えている場合は、複数の圧縮ファイルに分割されます。

（注） ファイル名の拡張子 *.zip* は変更しないでください。zip で圧縮されたファイルを解凍すると、拡張子 .gz が含まれていることがあります。

[Log Collection Jobs] ペインの下の [Delete] ボタンを使用してジョブを削除することができます。

これらのジョブは [ジョブ管理（Job Management）] ページ（**[システム管理（System Administration）]** > **[ジョブ管理（Job Management）]**）にも一覧で表示されますが、このページからログ ファイルをダウンロードすることはできません。

（注） ログ収集ジョブの詳細が必要な場合は、https://<ip-address>/emsam/log/Troubleshoot/LogCollectionManagerImpl.log を参照してください。<ip-address> には、Cisco Prime Collaboration Assurance サーバの IP アドレスを指定します。この URL は管理者ロールを持つユーザが表示することが可能で、ログ収集に関する問題をトラブルシューティングする場合に役に立ちます。



第 30 章

コール シグナリングの分析

このセクションでは、次の点について説明します。

- コール シグナリングの分析 （693 ページ）
- サポートされるコール フロー （696 ページ）
- コール ラダー ダイアグラムの作成 （697 ページ）
- コール ラダー ダイアグラムのメッセージのフィルタリング （700 ページ）
- コール ラダー ダイアグラムについて （700 ページ）

コール シグナリングの分析

SIP Call Flow Analyzer を使用すると、コールが失敗した原因を特定することができます。SIP Call Flow Analyzer はコールの概要を分析し、同じツールを使用してコンポーネント内の細かいレベルまでドリル ダウンします。

SIP Call Flow Analyzer を使用すると、次のことができます。

- コールの発信者、中間の宛先、および最終的な宛先が含まれているシグナリング パスの概要を表示し、コールの完全パスを理解できるようにします。
- シグナリングのコール ラダー ダイアグラムを表示し、コール内の問題を分離します。
- コール内の個々のコンポーネントにドリル ダウンしてエラーを修正します。
- エラー メッセージ、考えられる根本原因、および推奨事項を表示します。
- シグナリング エラーおよび機能の不整合を自動で特定し、強調表示します。
- Unified CCE のログを追加して、Unified CCE の導入に対してコール ラダー ダイアグラムを生成します。

Unified Communications の次のコンポーネントから取得したコール ログを分析します。

デバイス タイプ	**Advanced** モードでサポートされているリリース	コンポーネントまたはログのタイプ
Cisco Unified Contact Center Enterprise（Unified CCE）	9.x 以降	ルータ
Cisco Voice Portal（CVP）	9.x 以降	すべて

デバイス タイプ	**Advanced** モードでサポートされているリリース	コンポーネントまたはログのタイプ
Cisco Unified Communications Manager（Unified CM）	9.x 以降	コール ログと SDL ログ
IOS ゲートウェイ（TDM、CUBE（Enterprise Edition）、VXML GW）	15.1(4)M 以降	show logging コマンドの出力

前提条件

- Unified CCE および CVP デバイスのコール ログを分析するには、Contact Center Assurance ライセンスを追加する必要があります。ただし、Unified CM ではこの機能を継続して使用することができます。
- Cisco Prime Collaboration Assurance のデバイスの設定についての詳細は、次の場所にあるリストを参照してください。
  - Cisco Prime Collaboration Assurance のデバイス設定
  - Cisco Prime Collaboration Assurance のデバイス設定
- 次のセクションで説明されている設定を完了していることを確認します。
  - Unified CCE に対するデバッグ レベル 3 の設定：「Configure Debug Level 3 for UCCE Using System CLI」
  - CVP に対するデバッグ レベル 3 の設定：「Configure Debug Level 3 for CVP Using System CLI」
  - IOS ゲートウェイの設定：「Configure IOS Gateway」

（注）

- Advanced モードではサポートされているどのデバイス（Unified CM、CVP、IOS ゲートウェイ、Unified CCE）からでもログの分析ができますが、
- SIP over TCP のメッセージのみが解析されます。
- Unified CM：SDL/SDI とコール ログの両方が使用できる場合、SDL/SDI ログからコールが解析されます。SDL/SDI ログのデータが利用できない場合は、コール ログが使用されます。
- System CLI ツール、または別の Cisco Prime Collaboration Assurance サーバ 11.0 から収集したログのみがサポートされています。
- デバイスのタイム ゾーンは System CLI ツールからは収集されません。
- Contact Center Assurance ライセンスの有効期限が切れた場合、SIP Call Flow Analyzer は Contact Center のデバイス（UCCE、CVP）から受信したログの分析ができなくなります。ライセンシングの詳細については、『Cisco Prime Collaboration Assurance Guide-Advanced』の「*Manage Licenses*」の章を参照してください。
- オペレータおよびヘルプデスク ユーザはデバイスからコール ログを収集できません。また、シグナリング コール ラダー ダイアグラムと **SIP Call Flow Analyzer** のメニュー ページへアクセスすることもできません。

この機能の要件およびサポートされる内容は次のとおりです。

この機能に必要な最大ディスク サイズ。	小規模のプロファイル場合は 18 GB、中規模および大規模のプロファイルの場合は 35 GB。
インポート可能な最大ファイル サイズ。	小規模のプロファイルの場合は 0.5 GB、その他のプロファイルの場合は 1 GB。
ラダーの生成で一度に選択できるコールの最大数。	25
同時にログ収集対象にできるデバイスの最大数。	100
1 つのインスタンスで解析できる zip 形式のログ ファイルの最大サイズ。	小規模のプロファイルの場合は 0.5 GB、その他のプロファイルの場合は 1 GB。 （注） このサイズには、すべてのデバイスとコールが含まれています。zip ファイルのサイズが上記のサイズを超えると、ログは複数の zip ファイルに分割されます。小規模のプロファイルの場合は 0.5 GB のファイルに、その他のプロファイルの場合は 1 GB のファイルに分割されます。
ユーザ インターフェイスに表示されるコール レコードの最大数。	10,000

同時にサポートされるジョブの最大数。	一度に実行できる分析ジョブは 1 つだけです。
1 つのログ ファイルの分析を実行するための時間。	これはファイルのサイズによって異なりますが、1 GB の 1 つのファイルに対して約 2 時間と推定されます。

サポートされるコール フロー

コール トレース機能により、SIP ベースのコールを分析することができます。

（注） 同じコールのすべてのコール レッグの分析（エンドツーエンドのコール分析）の相関関係は、コール フロー 1 と 2 のみでサポートされます。これらのコール（コール フロー 1 と 2）に対するエンドツーエンドのコール分析をサポートするには、異なる製品間で CISCO-GUID（SIP Message プロパティ）を同じにする必要があります。エンドツーエンドのコール分析は、コール フロー 1 および 2 以外の他のコール フローではサポートされません。

次のコール フローをサポートします。

図 *20 :* コール フロー *1*

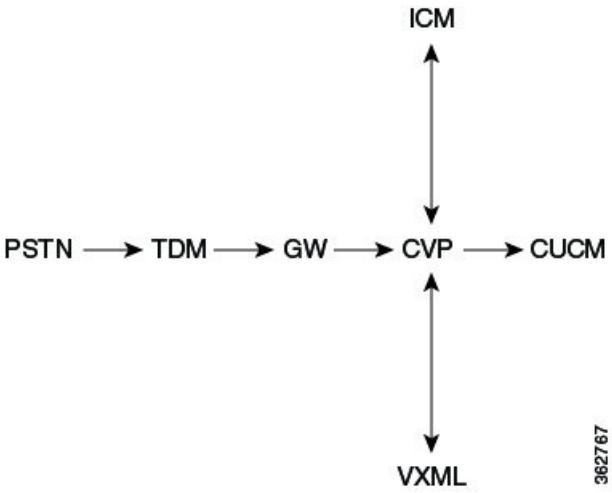


図 *21 :* コール フロー *2*

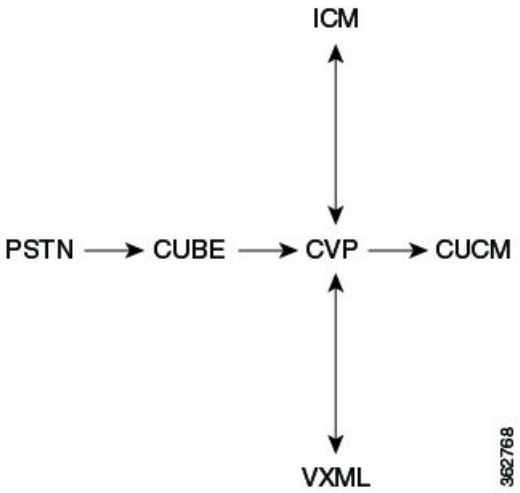


図 *22 :* コール フロー *3*

図 *23 :* コール フロー *3 A*

図 *24 :* コール フロー *4*

図 *25 :* コール フロー *5*

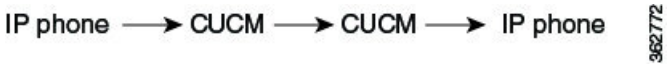


図 *26 :* コール フロー *5 A*

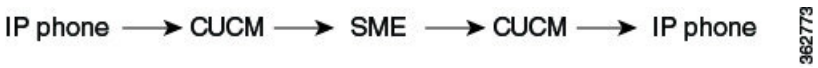
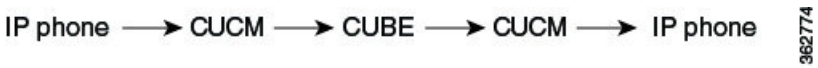


図 *27 :* コール フロー *6*



コール ラダー ダイアグラムの作成

ステップ 1 データ ソースを選択します。次のオプションから選択します。

- [Live Log Collection]：[Group Type] フィールドが表示されます。ドロップダウン矢印をクリックし、[Device Group] ダイアログボックスからデバイス グループを選択します。選択したデバイス グループで使用できるデバイスが表示されます。一覧されるオプションからデバイスを選択します。

  （注） 1 つまたは複数のデバイスを選択できます。

- [Local File System]：表示されるオプションからログ ファイルを選択できます。これには、デバイス ログ コレクタ や、ライブ ログ コレクションから収集されたログファイルも含まれます。また、[Import] をクリックしてローカル ファイルからファイルをインポートできます。[Import] ダイアログボックスで、zip されたログ ファイルを参照します。 導入のモードに基づいて、[Import] ダイアログボックスの [domain/customer] ドロップダウン リストを使用して、カスタマーまたはドメインをインポートされたログに関連付けることができます。インポートされたファイルは、[Log File System] の下で使用できるオプション内で更新されます。デバイス ログ コレクタの詳細については、ログ収集センター/デバイス ログ コレクター （686 ページ）を参照してください。[Export] ボタンを使用してログ ファイルをエクスポートすることもできます。

インポートについては、.gz、.gzo、および .zip の各ファイル形式がサポートされています。エクスポートされるファイルも .gz、.gzo、および .zip ファイル形式です。接続できるログ ファイルは 1 つだけです。zip で圧縮されたファイル サイズが（小規模のプロファイルで）0.5 GB を超えている場合、または（中規模または大規模のプロファイルで）1 GB を超えている場合は、インポート タスク用に、（小規模のプロファイルで）0.5 GB、（中規模または大規模のプロファイルで）1 GB の複数のファイルに分割されます。

ログ ファイル システムを選択した場合は、ログ ファイルの削除もできます。フォルダおよび処理したレコードのクリーンアップに時間がかかるため、このタスクの完了には長時間かかる場合があります。

ステップ 2 （オプション）[Filter Calls]：次のパラメータを使用して、前述のデータ ソースから、選択したファイルのコールを検索します。

Cisco Prime Collaboration リリース 12.1 SP3 以降の場合

（注） ライブ ログの収集の間に、[発信番号/URI（Calling Number/URI）] フィールドを使用して、結果をフィルタリングすることができます。これは、発信者番号/URI、着信者番号/URI、コール ID、および GUID のフィールドに適用されます。検索を実行する前に、次のガイドラインに従っていることを確認してください。

- 発信番号の 1 桁以上の番号を指定します。
- 「*」などの特殊文字は検索に使用できません。

Cisco Prime Collaboration リリース 12.1 SP3 以降の場合

フィールド	説明
Calling Number/URI	SIP-URI は、SIP を介して他の人をコールするための SIP のアドレッシング スキーマです。デフォルトでは [ALL] が表示されます。
Called Number/URI	デフォルトでは [ALL] が表示されます。
Disconnect Code	コールのエラー コード（200 OK など）。
Call ID	1 つの Cisco UC 製品内でコールを一意に識別する ID。コールの各コール レッグには異なる コール ID があります。

GUI ID	複数の製品間でコールを一意に識別する ID。
Time Zone	デフォルトでは、Cisco Prime Collaboration Assurance サーバのタイムゾーンが表示されます。
Heartbeat Messages	ハートビート メッセージ OPTIONS および NOTIFY が含まれます。このフィールドを選択すると、この機能のパフォーマンスが低下することがあります。
時間範囲	時間の範囲を指定できます。[Local File System] を選択した場合、過去の時間の詳細オプションは使用できません。コールが発生した時間範囲を選択するようにしてください。
パースするデバイス タイプ	選択したログに含まれているデバイス タイプがここに一覧されます。特定のデバイス タイプを選択して、そのデバイス タイプが含まれているコールをフィルタリングすることができます。
コールの最大数	デフォルトでは、この値は 500 に設定されます。値を大きくすると、レコードの表示に時間がかかることがあります。したがって、適切なフィルタを設定することをお勧めします。
Initial Message	デフォルトでは、[Initial Message] は INVITE（特定のコール ID に対するコールの最初のメッセージ）として選択されます。[Initial Message] として別の値を選択することもできます。
Comment	ログが収集されるタイミング、場所、および理由を表すコメントを追加できます。

ステップ 3 [Retrieve Calls] ボタンをクリックします。[Live Log Collection] オプションを選択した場合、[Log Parsing In Progress] ステータス バーが表示されます。ログの解析処理が完了すると、[Log Download In Progress] ステータス バーが表示され、処理が完了したことが示されます。[Local File System] オプションを選択した場合、すぐに [Log Download In Progress] ステータス バーが表示されます。アップロードしたログ ファイル、または既存のログ ファイルを解析しようとしても、ファイルはすでに解析されているため、[Log Analysis In progress] ステータス バーは表示されません。

IOS ゲートウェイと Unified CM コールのログには、古いデータが含まれている可能性があります。特定の期間のコール リストを取得するには、適切なフィルタを適用する必要があります。

[Local File System] オプションの場合は、ファイルは最初に解凍され、解析されてから、分析されます。

[Live Log Collection] オプションの場合は、ファイルは最初にダウンロードされ、解凍、解析されてから、分析されます。

ステップ 4 コール リストが表示されます。このリストからコールを選択し、表示されたコールについて [Show Ladder Diagram] をクリックします。[Call Ladder diagram] ページが表示されます。

新しいタブにコール ラダー ダイアグラムが表示されます。

（注） コールプロセッサ（導入環境内の Unified CM）を使用している場合は、コールの各コール レッグに異なるコール ID が付けられます。そのため、完全なコールのコール ラダー ダイアグラムを表示するには、[Call List] からすべてのコール レッグを選択し、[Show Ladder Diagram] ボタンをクリックします。

コール リストが表示されているときに [Show Transition Diagram] ボタンをクリックすることにより、コールのメッセージ遷移を表示することもできます。Unknown エラーは Unexpected エラーと同じです。

図 *28* : 遷移ダイアグラム

コールが表示されない場合は、次の内容を確認します。

- フィルタが正しく適用されている。
- 選択したタイム ゾーンの範囲が、実際のデバイスのタイム ゾーンと一致している。
- 機能を使用する前に、デバイスで適切なデバッグ レベルが設定されていた。Cisco Prime Collaboration Assurance Collaboration のデバイスのセットアップとデバイスの設定のリストに関しては、次のリンク先を参照してください。
  - Cisco Prime Collaboration Assurance のデバイス設定
  - Cisco Prime Collaboration Assurance のデバイス設定

コールラダーダイアグラムのメッセージのフィルタリング

特定のメッセージについてコール ラダー ダイアグラムを作成することができます。

ステップ 1 コール ラダー ダイアグラムのメッセージを次のパラメータでフィルタリングすることもできます。

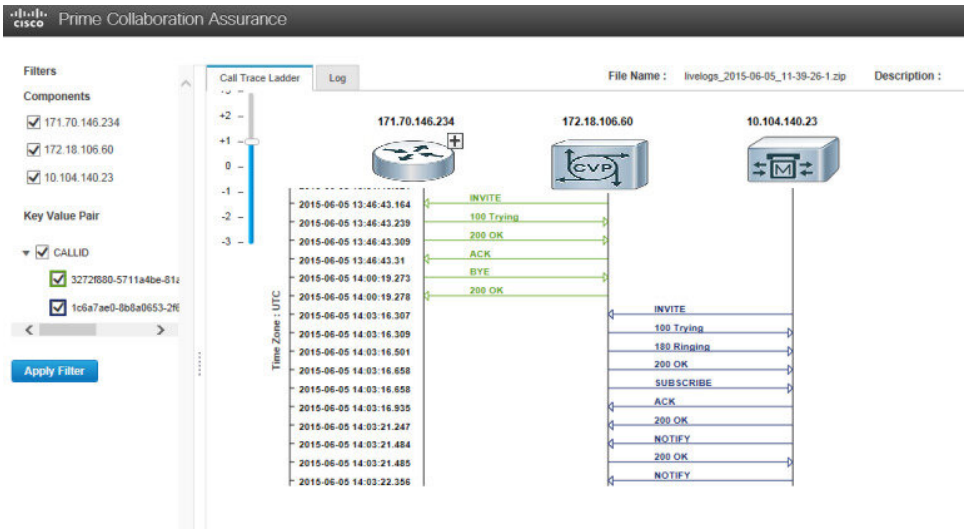
- [Components]：コール内のデバイスの IP アドレス（送信者および受信者）。
- [Key Value Pair]：コールの属性。これには、Call ID と GUID が含まれます。

ステップ 2 パラメータを選択して [Apply] をクリックします。適用したフィルタに従ってダイアグラムが生成されます。

コール ラダー ダイアグラムについて

コールラダーダイアグラムは、選択したコールの（回線側とトランク側の両方の）SIP シグナリングを視覚化する場合に便利です。

図 *29* : コール ラダー ダイアグラム



次の内容を表示することができます。

- メッセージの方向
- 送信者と受信者
- 個々のメッセージのタイム スタンプ。コール ラダー ダイアグラムには UTC タイム ゾーンのみが表示されます。
- メッセージとメッセージ ラベル。メッセージの矢印をクリックすると、[Call Details] ポップアップ ウィンドウが起動してコールの詳細が示されます。次を実行できます。
  - コールの詳細を表示する。
  - このウィンドウでコール ID をフィルタリングする。
  - デバイスのタイム スタンプとタイム ゾーンを表示する。このタイム スタンプは UTC に変換され、表示されます。
  - **[Click here for log]** をクリックし、クリックした（黄色で強調表示された）メッセージのログ スニペットを表示する。

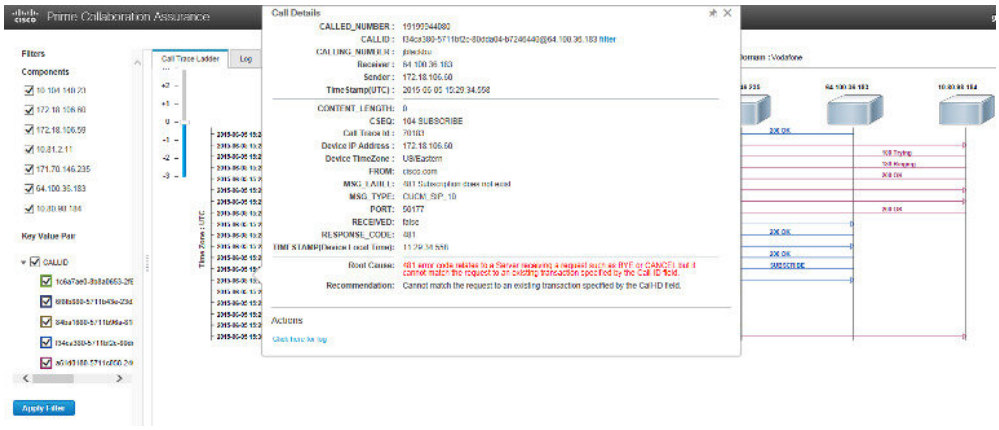
[Logs] タブをクリックして、選択したメッセージのログ スニペットを表示することができます。最初にクリックしたときには、ログは表示されません。

（注） デフォルトでは、[Call Details] ポップアップ ウィンドウの **[Click here for log]** ボタンをクリックすると、選択した最後のメッセージのログ スニペットが表示されます。特定のメッセージのログを表示するには、コール ラダー ダイアグラムでメッセージの矢印をクリックして [Call Details] ポップアップ ウィンドウを表示します。ここで **[Click here for log]** ボタンをクリックします。

（注） ログにデバイス タイプの詳細がない場合は、コール ラダー ダイアグラムに、マークのないグレーのデバイス アイコンが表示されます。これは、デバイスが不明であることを表します。

ダイアログを作成するときに [Device Types to Parse] フィールドで特定のデバイスのみを選択してコールをフィルタリングすると、コールのコンポーネント（[Device Types to Parse] フィールドで選択されていないデバイス）が示されて、コールをトラブルシューティングする場合に役に立つことがあります。そのデバイスに関するログが解析、表示され、デバッグに使用することができます。これらのデバイスには、プラス記号のアイコンが表示されます。プラス記号をクリックして、コール ラダー ダイアグラムを展開します。点線は、新しいコンポーネントが拡張の一部として追加されたことを表します。メッセージのタイム スタンプの順序に基づいて、デバイスの並べ替えが行われることもあります。

図 *30 : [Call Details]* ポップアップ ウィンドウ



コールにエラーがある場合、メッセージの矢印が赤で表示されます。矢印をクリックし、[Call Details] ポップアップ ウィンドウを開いてエラーの根本原因や推奨事項を確認して、コール障害の原因のトラブルシューティングに有効に使用することができます。

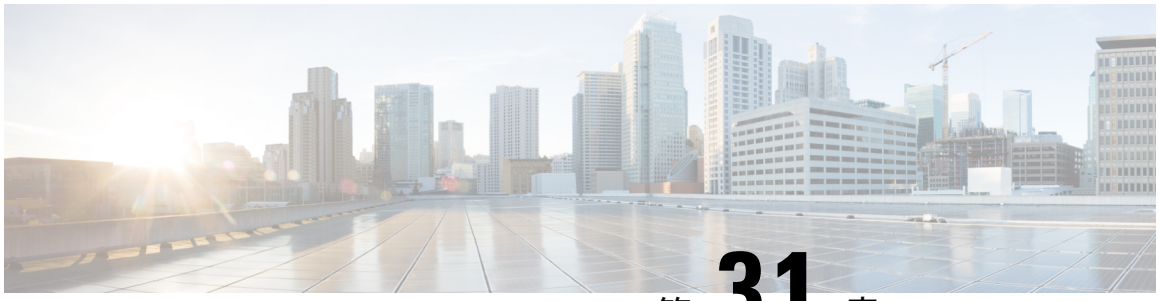
各コール ID は異なる色で表示され、スキーマはダイアグラムの下に示されます。

ダイアグラムのズームインとズームアウトができます。

第 IX 部

サーバの保守

- ジョブの管理 （705 ページ）
- パージ ポリシー （713 ページ）
- バックアップと復元の実行 （717 ページ）
- ログ レベルの設定 （725 ページ）



第 31 章

ジョブの管理

このセクションでは、次の点について説明します。

- ジョブの管理 （705 ページ）

ジョブの管理

Cisco Prime Collaboration Assurance を使用すると、[ジョブ（Jobs）] ペインですべての即時ジョブおよび定期ジョブの詳細を表示できます。手動でスケジュールされるジョブは、検出、インベントリ更新、会議インポートです。ポーリング ジョブは、ユーザ設定値に基づいて、トリガーされます。

表 97 : Job Details [ジョブ管理（Job Management）] ページ（に表示されるフィールドの説明を示します。**[システム管理（System Administration）] > [ジョブ管理（Job Management）]**。最新情報を取得するには、ページを更新します。

表 97 : Job Details

フィールド	説明
Name	Cisco Prime Collaboration Assurance で定義されたジョブの説明です。
Type	ジョブのタイプを示します。
Description	ジョブの説明です。

フィールド	説明
Status	ジョブのステータスです。次のいずれかになります。 • Completed：ジョブが完了しました。ジョブが完了しても、成功したとは限りません。ジョブがいくつかのデバイスで失敗している可能性もあります。ジョブの詳細は、ページの左端にある矢印をクリックして [Job Instances] テーブルで表示できます。 • Cancelled：ジョブがキャンセルされました。スケジュール済みジョブをキャンセルできます。ただし、実行中のジョブまたはシステム ジョブ（たとえば、ポーリング ジョブ）はキャンセルできません。 • Scheduled：ジョブは、特定の時刻に実行されるようにスケジュールされています。ジョブは一度で実行されるか、または複数回繰り返し実行されるようにスケジュールできます。 • Suspended：ジョブは一時的に停止されました。後で実行を再開できます。 • Running：ジョブが実行中です。
Owner	ジョブを作成したユーザです。事前定義されたシステム ジョブの場合、[Creator] には [SYSTEM] と表示されます。
Job Start Time	ジョブが最初に実行をスケジュールされている時刻。
Job End Time	ジョブがアクティブになっている時間です。スケジュールされているすべてのジョブのインスタンスを実行したら、ジョブは非アクティブになります。
Next Scheduled Time	以降のジョブ インスタンスの開始時刻です。これは、定期的に繰り返されるジョブに適用されます。即時ジョブまたはワンタイム ジョブのいずれかの場合、[Job Start Time] および [Next Scheduled Time] に表示される時刻は同じです。

フィールド	説明
Schedule Type	ジョブが定期的または一度実行するようにスケジュールされているか示します。
[Job Details] ペイン	
Run ID	定期ジョブの場合、ジョブインスタンス カウントが表示されます。定期ジョブではない場合、ゼロを表示します。
Status	同じジョブのジョブ インスタンスのステータスです。この列のクイック ビュー アイコンにマウスを合わせると、ジョブ インスタンス結果が表示されます。
Status Progress	ジョブの段階と、完了率を示します。
Results	ジョブが成功したか、失敗したかを示します。
Start Time	同じジョブのジョブ インスタンスの開始時刻です。
End Time	同じジョブのジョブ インスタンスの終了時刻です。
Duration	同じジョブのジョブ インスタンスの開始時刻と終了時刻との間で経過する時間です。

（注） パージ ポリシーの詳細については、「パージ ポリシー テーブル （713 ページ）」を参照してください。

ジョブをスケジュールする

[ジョブの詳細（Job Details）]ペインの[スケジュールと設定（Schedule and Settings）]タブで、ジョブのスケジュールやオプションの設定ができます。

（注） スケジュールと設定のタブは、検出ジョブに対してのみイネーブルになります。検出ジョブをスケジュールできるのは、[インベントリ管理（Inventory Management）]ページのみです。[ジョブ管理（Job Management）] では、ジョブのスケジュールはできません。

次のいずれかのステータスを持つ検出ジョブのスケジュールのみを変更できます。

- スケジュール済み

- 不合格

ジョブをスケジューリングする手順は次のとおりです。

ステップ 1 [ジョブ（Jobs）] ペインでジョブを選択し、[詳細（Details）] ペインの [スケジュール（Schedule）] タブをクリックします。

ステップ 2 [Schedule Options] で、開始時刻、終了時刻、繰り返しを選択します。

[Daily]、[Weekly]、[Monthly] のいずれかの繰り返しを設定し、日付と頻度を指定します。必要に応じてジョブを数時間おきにスケジューリングするには、[Hourly] を選択する必要があります。

スケジュールが定義されます。繰り返しを [None] に設定すると、他の頻度の詳細を指定できません。

次のタイプの定期的な間隔を設定できます。

表 *98* : 定期的な間隔のタイプとスケジュール

定期的な間隔のタイプ	スケジュール
なし	他の周波数の詳細を指定することはできません。
毎時	ジョブは、指定した開始時刻に最初に開始され、その後、指定した間隔、つまり、指定した数時間ごと（日、時、分）に開始されます。
毎日	ジョブは 1 日に 1 回実行されます。 ジョブが毎日 HH:MM の形式で指定された時刻に開始することを意味します。 日ごとの時間間隔では、スケジューラは毎日指定した時間に開始時刻を想定して実行されます。
毎週	ジョブは 1 週間に 1 回実行されます。 ジョブが週の指定された曜日に開始することを意味します。 曜日を指定する際は、1 は日曜日、2 は月曜日というように、整数を 1 つ選択して指定します。 たとえば、スケジューラは、毎週金曜日（選択した曜日が金曜日の場合）の指定した時刻に開始することを想定しています。

定期的な間隔のタイプ	スケジュール
毎月	ジョブは月に 1 回実行されます。 各月の指定された日にジョブを開始することを示します。 月の1 週目、2 週目、3 週目、または 4 週目のいずれかを指定すると、ジョブは毎月特定の曜日に開始されます。 たとえば、月間隔で設定すると、スケジューラは、毎月特定の週の特定の日の特定の時間に開始することを想定します。

ステップ 3 **[設定（Settings）]** タブをクリックし、オプションの選択に進みます。

定義した設定に従ってジョブが実行されます。このジョブのステータスは、[Jobs] ペインで [Scheduled] に設定されます。

（注） CMEPhoneDiscovery および PhoneXML の探索ジョブは、4 時間ごとに定期的な間隔でスケジュールされます。繰り返しが [なし（None）] に設定されている場合は、これをスケジュールに戻すことはできず、Cisco Prime Collaboration Assurance を再起動する必要があります。

ステップ 4 [保存（Save）] をクリックします。

タイムテーブルの定義

1つまたは複数のジョブで使用するタイムテーブルをスケジューラで定義できます。スケジューラは現在の時刻を考慮します。

たとえば、現在の日付と時刻が「2017/06/23、13:48:00 IST」の場合、ジョブは次のように開始されます。

スケジューラ
開始時間：2017/06/20 06:27 PM
繰り返し：時間
毎時：5 時間
ジョブの開始時間：2017-Jun-20 13:27:00 IST
次のスケジュール時間：2017-Jun-20 15:27:00 IST

ジョブは [ジョブの開始時間（Job Start Time）] に 1 回実行します。

次のスケジュール時間は、[Start Time（開始時間）] とは関連しません。時間数をかけた時刻に開始します。このジョブの次のスケジュール時間のシーケンスは、次のとおりです。

1. 2017-Jun-20, 15:27 時間（次のスケジュール時間）
2. 2017-Jun-20, 20:27 時間 (15:27 + 5)
3. 2017-Jun-21, 00:27 時間（時刻は 00:27 時間にリセット）
4. 2017-Jun-21, 05:27 時間 (00:27 + 5 = 05:27)
5. 2017-Jun-21, 10:27 時間（05:27 + 5 = 10:27）

（注） スケジューラは、1 つ前のジョブが完了しない限り、次のジョブを開始しません。

たとえば、ジョブを 22:00 から開始し、1 分間隔で完了するようにスケジュールしたとすると、ジョブの完了には 2 分かかります。スケジューラは 最初のジョブを 22:00 に開始し、実際には 00:02 に完了します。

ジョブのキャンセル

[ジョブのキャンセル（Cancel Job）]を使用し、**スケジュール済み**状態にある検出ジョブを取り消すことができます。ただし、ステータスが次のいずれかの場合、ジョブはキャンセルできません。

- キャンセル済
- 完了
- 失敗
- 実行中

また、次のジョブはキャンセルできません。

- Polling：*Polling* という単語で始まるすべてのジョブ。Polling_CTS-HEALTH_、Polling_TelepresenceSystem_、Polling_CtsMAN-HEALTH_ など。
- Purging：*Purging* という単語で始まるすべてのジョブ。

事前定義済みのクイック フィルタ

Cisco Prime Collaboration Assurance は、次の定義済みのクイック フィルタをサポートしています。

- [All Discovery Jobs]：検出ジョブの例は DiscoveryFrmBackgroundPathtrace です。デバイスの検出や再検出の実行時、またはインベントリ タスクの更新時に、

  Cisco Prime Collaboration リリース 11.5 以降の場合

  [インベントリ（Inventory）] > [インベントリ スケジュール（Inventory Schedule）] > [IP フォン インベントリ スケジュール（IP Phone Inventory Schedule）]。

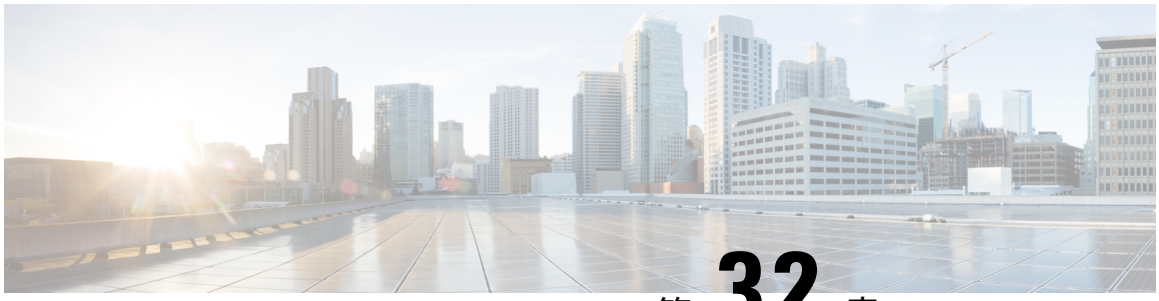
ジョブ インスタンスの結果を表示する：[ジョブの詳細（Job Details）] ペインの [実行ID（Run ID）] 列の値にマウス ポインタを合わせてから、[クイック ビュー（Quick View）] アイコンをクリックすると、[全体のデバイス サマリー（Total Device Summary）] と [エンドポイント デバイスのサマリー（Endpoint Device Summary）] を表示できます。

- すべてのポーリング ジョブ：ポーリング ジョブの例として、MCU_Conference_Import があります。ポーリング ジョブは、システムが設定された時点で自動的に作成されます。
- [All Report Jobs]：レポート ジョブは、レポートが実行されると一覧に示されます。
- すべてのポーリング ジョブ：セッション インポート ジョブの例は MNGD_Synch_CtsMAN-MEETING です。セッションは、 Cisco TMS からインポートされます。これらの管理アプリケーションごとに、個別にジョブが作成されます。
- **Cisco Prime Collaboration リリース 11.5 以降の場合**

  すべての会議インポート ジョブ：会議インポート ジョブの例は、MNGD_Synch_TMS-MEETING です。会議は、Cisco TMS からインポートされます。これらの管理アプリケーションごとに、個別にジョブが作成されます。
- [All System jobs]：検出、ポーリングなどのシステム生成ジョブ。システム生成ジョブは、システムがジョブを実行するとすぐに一覧に示されます。
- [All User Jobs]：ユーザ ジョブの例は RediscoverDevices_1347339631540 です。ユーザ ジョブは、ユーザがジョブを実行するとすぐに一覧に示されます。
- [Jobs Run in Last 24 Hours]：過去 24 時間に実行されたジョブの例は、Discovery 2012-Sep-13 10:32:40 UTC です。最後に完了した時間（最後の実行インスタンス）が（現在の時刻から）過去 24 時間以内に収まるすべてのジョブを一覧に示します。

関連トピック

デバイスの検出



第 32 章

パージ ポリシー

このセクションでは、次の点について説明します。

- パージ ポリシー （713 ページ）
- パージ ポリシー テーブル （713 ページ）

パージ ポリシー

Cisco Prime Collaboration Assurance では、次のパージ ポリシーを使用しています。

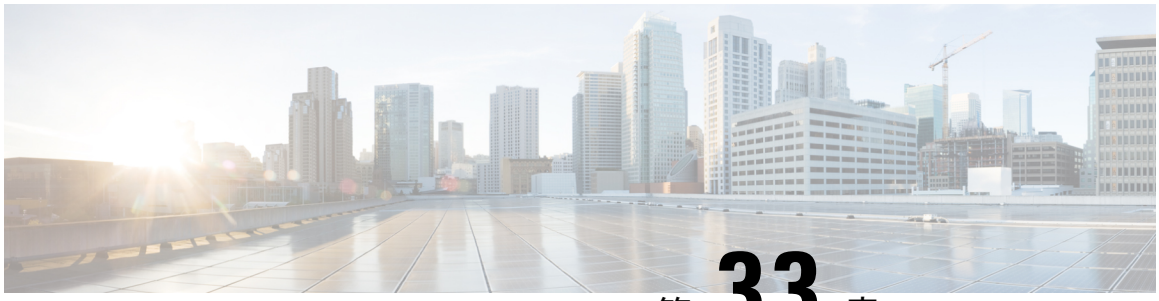
パージ ポリシー テーブル

表 *99* : パージ ポリシー テーブル

モジュール	パージ ポリシー
障害のモニタリング	クリアされたアラームは、30 日間（4 週間）でパージされます。 イベントは 60 日間（8 週間）でパージされます。
	アラームがパージされると、すべての関連イベントもパージされます。アクティブなイベントとアラームはパージされません。
	あるデバイスのいずれかのパフォーマンス カウンタに対するしきい値ルールがパージされると、関連するアクティブなアラームもパージされます。

モジュール	パージ ポリシー
ネットワークの監視	1 日以上経過したすべての会議のエンドポイント統計データはパージされます。
	14 日以上経過したすべてのセッションおよびトラブルシューティング情報は、1 時間ごとにパージされます。 **Cisco Prime Collaboration リリース 11.1 以前の場合** 14 日以上経過したすべての会議情報は 1 時間ごとにパージされます。
ダッシュボード	30 日以上経過したコール品質のイベント履歴、および音声/ビデオ電話の監査レポート データはパージされます。 **Cisco Prime Collaboration リリース 12.1 以降の場合** 30 日以上経過したコール品質イベント履歴とエンドポイントに関連する監査レポート データは削除されます。
	7 日より古い CDR レポートはパージされます。
	7 日より古い CMR レコードはパージされます。
	センサーのデータで、7 日より古いものはパージされます。
	Cisco Prime NAM/vNAM のデータで、7 日より古いものはパージされます。
	パフォーマンス ダッシュボードが 30 分以上開いていない場合は、次にカスタム ダッシュボードが起動されるときにキャッシュ メモリがパージされます。
	カスタム ダッシュボードのカウンタに対して履歴トレンド オプションが無効になっている場合、またはダッシュボードが削除されている場合は、データベース内のポーリングされたすべてのデータがパージされます。
診断の実行	IP SLA Voice テスト データ - Cisco Prime Collaboration Assurance は、31 日以上経過したすべてのデータ ファイル（保存されたテスト データ）をパージします。31 日以上経過したデータを保持するには、テストを別のサーバで保存する必要があります。

モジュール	パージ ポリシー
サーバの保守	14 日以上経過しており、ステータスが完了済み、失敗、またはキャンセルのジョブは、1 時間に 1 回パージされます。
	イベントおよびアラームデータベース - アクティブおよびクリアされたすべてのイベントとアラームは、Cisco Prime Collaboration Assurance データベースに保管されます。イベント間の関係は保存されます。アラームおよびイベント ブラウザではデータベースの内容を確認できます。このデータの消去間隔は 4 週間です。
ジョブ管理	32 日より古いジョブはパージされます。



第 33 章

バックアップと復元の実行

このセクションでは、次の点について説明します。

- バックアップと復元の実行 （717 ページ）

バックアップと復元の実行

Cisco Prime Collaboration Assurance のユーザインターフェイスを使用して、定期的なバックアップをスケジュール、

Cisco Prime Collaboration Analytics データは、SSH を使用してリモート サーバ上にバックアップされます。これは Cisco Prime Collaboration Assuranceのバックアップ リポジトリを使用しません。分析データは、ユーザインターフェイスを使用してのみバックアップでき、CLI を介してデータを復元することができます。

（注） Cisco Prime Collaboration Analytics のバックアップ用には Linux サーバが推奨されています。

Cisco Prime Collaboration Analytics は Windows サーバでバックアップすることもできます。および Cygwin UNIX シェルのみを使用して提供されます。Windows サーバのバックアップ サポートでは、その他の SSH ツールまたは Unix シェルを使用することはできません。

関連トピック

会議の監視

ビデオ エンドポイントのトラブルシューティング ワークフロー （657 ページ）

パージ ポリシー （713 ページ）

概要 （43 ページ）

バックアップと復元の概要

Cisco Prime Collaboration Assurance では、次のパージ ポリシーを使用しています。

- 1 日以上経過したすべての会議統計とエンドポイント統計データはパージされます。

- **Cisco Prime Collaboration リリース 11.5 以降の場合**

  14 日以上経過したすべての会議およびトラブルシューティング情報は、1 時間ごとにパージされます。

- **Cisco Prime Collaboration リリース 11.6 以前の場合**

  30 日以上経過したコール品質のイベント履歴および音声/ビデオ電話の監査レポート データは、パージされます。

  Cisco Prime Collaboration リリース 12.1 以降の場合

  30 日以上経過したコール品質イベント履歴とエンドポイントに関連する監査レポート データは削除されます。

- 14 日以上経過したクリア済みアラームおよびイベントは、1 時間に 1 回パージされます。アラームがパージされると、すべての関連イベントもパージされます。アクティブなイベントとアラームはパージされません。
- 14 日以上経過しており、ステータスが完了済み、失敗、またはキャンセルのジョブは、1 時間に 1 回パージされます。

バックアップと復元サービスを使用して、データベース、コンフィギュレーション ファイル、ログ ファイルをリモート ロケーションとローカル ディスクのいずれかにバックアップできます。バックアップ サービスでバックアップされるのは次のフォルダのファイルです。

Assurance バックアップのデータ タイプ
Assurance データベース
コンフィギュレーション ファイル

Analytics バックアップのデータ タイプ
Analytics データベース
ログ ファイル
レポート（スケジュール済みレポートとカスタム レポート）
ロゴ

バックアップ期間

Cisco Prime Collaboration Assurance サーバが管理する対象デバイスの数に応じて、データ バックアップの所要時間は次のとおりとなります。

- 最大 150,000 エンドポイント：4 時間
- 最大 80,000 エンドポイント：2.5 - 3 時間
- 最大 20,000 エンドポイント：2 時間

- 最大 3,000 エンドポイント：1 時間

Note ネットワーク遅延が 20 ms を超えると、上記の時間を満たすことができません。

バックアップをスケジュールする場合、この操作によって Cisco Prime Collaboration Assurance のユーザインターフェイスのパフォーマンスが低下する可能性があるため、業務時間外を推奨します。

FTP、ディスク、SFTP、または TFTP サーバでのリポジトリの作成

Cisco Prime Collaboration のデータをバックアップする前に、リポジトリを作成する必要があります。デフォルトでは、バックアップ サービスは *.tar.gpg ファイルを設定されたリポジトリに作成します。バックアップされたファイルは圧縮形式になっています。CD-ROM、ディスク、HTTP、FTP、SFTP または TFTP にあるリポジトリを使用できます。

ステップ 1 インストール中に作成したアカウントを使用して Cisco Prime Collaboration サーバにログインします。デフォルトのログインは *admin* です。

ステップ 2 次のコマンドを入力して、ローカルにリポジトリを作成します。

```
admin# config t admin(config)# repository RepositoryName admin(config-Repository)# url disk:
admin(config-Repository)# exit admin(config)# exit
```

次のコマンドを入力して、FTP サーバにリポジトリを作成します。

```
admin# config t admin(config)# repository RepositoryName admin(config-Repository)# url
ftp://ftpserver/directory admin(config-Repository)# user UserName password {plain | hash} Password
 admin(config-Repository)# exit admin(config)# exit
```

それぞれの説明は次のとおりです。

- *RepositoryName* とは、ファイルをバックアップする場所を指します。この名前には最大 30 文字までの英数字を指定できます。
- *ftp://ftpserver/directory* とは、FTP サーバおよびサーバ上のディレクトリで、ここにファイルを転送します。FTP の代わりに SFTP、HTTP、または TFTP を使用することもできます。
- ユーザ名と {**plain**|**hash**} パスワードは、FTP、SFTP、または TFTP サーバのユーザ名とパスワードです。**hash**で暗号化されたパスワードを指定し、**plain**で非暗号化されたプレーン テキストのパスワードを指定します。

  次に例を示します。

  ```
  admin# config t admin(config)# repository tmp admin(config-Repository)# url
  ftp://ftp.cisco.com/incoming admin(config-Repository)# user john password plain john!23
  admin(config-Repository)# exit admin(config)# exit
  ```

リポジトリ データの一覧表示

リポジトリ内のデータを一覧表示できます。Cisco Prime Collaboration サーバに *admin* としてログインし、次のコマンドを実行します。

```
admin# show repository RepositoryName
```

次に例を示します。

```
admin# show repository myftp assurance_Sun_Feb_09_14_20_30_CST_2014.tar.gpg
```

Cisco Prime Collaboration Assurance および Analytics ユーザ インターフェイスを使用したスケジュールのバックアップ

Cisco Prime Collaboration リリース 11.1 以前の場合

ユーザインターフェイスから Assurance および Analytics の両方にバックアップをスケジュールし、実行できます。

Cisco Prime Collaboration リリース 11.5 以降の場合

バックアップするには、管理者としてログインする必要があります。

新しいバックアップ ジョブを作成するには、次のようにします。

ステップ 1 選択 **[システム管理（System Administration）]** > **[バックアップ設定（Backup Settings）]**。

ステップ 2 [Backup] ページで [New] をクリックします。

ステップ 3 バックアップ ジョブの名前を入力します。

バックアップ名が指定されていない場合、[Backup Title] フィールドは、デフォルトにより日付スタンプに設定されます。

ステップ 4 ドロップダウン リストから [Backup Category] を選択します。

ステップ 5 [Assurance Connection Settings] ペインで次の詳細情報を入力します。

sFTP、FTP、またはローカル接続を使用してバックアップを作成できます。

[sFTP] または [FTP] を選択した場合は、次の詳細情報を入力します。

- バックアップ ファイルの格納先サーバの IP アドレス
- バックアップの場所へのパス バックアップは、

（注） 指定されたユーザ ホーム ディレクトリで実行されます。例としては、

フィールドの	[説明（Description）]
SSH ユーザ名	SSH のユーザ名を入力します。たとえば、「user1」または任意の名前を指定します。
[パス（Path）]	パスの名前を入力します。例としては、「/backup」などです。 その後、アシュアランスのバックアップの場所は /backup/assurance_backup になります。
バックアップは、/user1/backup/assurance_backup に保存されます。	

- ポート（sFTP の場合のみ）
- ユーザ名
- パスワード

クレデンシャルを使用して sFTP または FTP 接続をテストするには、[テスト（Test）] をクリックします。

ローカルを選択した場合は、ローカル マシンにバックアップ ファイルを保存する場所を指定します。

ローカル バックアップの場合は、[Backup History] ドロップダウン リストを使用して、保存するバックアップ ファイルの数を指定できます。デフォルトでは、最後の 2 個のバックアップ ファイルが保存されます。バックアップ ファイルは、最大 9 個まで保存できます。

[Analytics Connection Settings] ペインは、Cisco Prime Collaboration Analytics を有効にした場合のみ使用することができます。

Cisco Prime Collaboration リリース 11.5 以降の場合

Cisco Prime Collaboration Analytics は、MSP 展開でサポートされています。

ステップ 6 [Analytics Connection Settings] ペインで次の詳細情報を入力します。

SSH を使用して Analytics データをバックアップする場合は、リモート サーバのみ使用できます。

- バックアップ ファイルが保存されるリモート サーバの IP アドレス
- バックアップの場所へのパス。相対パスを指定する必要があります。

（注） バックアップは、指定したユーザのホーム ディレクトリで実行されます。例としては、

フィールドの	[説明（Description）]
SSH ユーザ名	SSH のユーザ名を入力します。たとえば、「user1」または任意の名前を指定します。
[パス（Path）]	パスの名前を入力します。例としては、「/backup」などです。 分析のバックアップ先は /backup/pg_basebackup となり、その後にタイムスタンプが続きます（例：pg_basebackup_201707201255）。
バックアップは /user1/backup に保存されます。	

Analytics のバックアップ フォルダは次の形式になります。pg_basebackup の後にタイムスタンプ（例：pg_basebackup_201707201255）。sFTP サーバ上にユーザが存在しない場合、バックアップは失敗します。

- SSH ポート
- SSH ユーザ名
- SSH パスワード

クレデンシャルを使用して接続をテストするには、[Test] をクリックします。

ステップ 7 バックアップ開始時刻および繰り返し間隔を指定します。

日付の選択に表示される時刻は、クライアント ブラウザの時刻です。

ステップ 8 （オプション）バックアップ ステータス通知の送信先となる電子メール ID を入力します。複数の電子メール ID はカンマで区切って指定します。

電子メールを受信するには、Cisco Prime Collaboration Assurance サーバ で SMTP サーバの詳細を（**[アラームとイベントの電子メール設定（E-mail Setup for Alarms & Events）]**）で設定します。

Cisco Prime Collaboration リリース 11.5 以降の場合

電子メールを受信するには、Cisco Prime Collaboration Assurance サーバ で SMTP サーバの詳細を（**[アラームおよびレポート管理（Alarm & Report Administration）]** > **[アラームおよびイベント用に電子メールをセットアップ（E-mail Setup for Alarms & Events）]**）で設定します。

ステップ 9 **[Save]** をクリックします。

スケジュール設定したバックアップ ジョブが [Backup Management] ページに一覧表示されます。

[Run Now] をクリックすると、即座にバックアップを実行できます。

トラブルシューティング

問題：Cisco Prime Collaboration Assurance のバックアップ ジョブのステータスが、レポートの生成後でもエラーと表示される。バックアップ ジョブが Cisco Prime Collaboration Assurance でスケジュールされている場合、バックアップ ファイルは sFTP ロケーションに生成され格納されます。この場所に、ゼロ以外のサイズのファイルが作成されます。Cisco Prime Collaboration Assurance でスケジュールされたジョブのステータスが、実行されるたびにエラーになります。

期待：ジョブがエラーにならないか、エラーの原因が存在してエラーになる必要があります。

Cisco Prime Collaboration Assurance のバックアップ ジョブのステータスが、sFTP にレポートが生成されるにもかかわらずエラーと表示されます。その場合は、バックアップ時に sFTP サーバのパスを変更してください。Cisco Prime Collaboration Assurance のレポートに使用する sFTP ロケーションに、非ルートのユーザ ロケーションを設定します。この問題の原因は、GPG キーがユーザ フォルダに存在しないことです。

バックアップに使用する sFTP ロケーションには、ルート ディレクトリ以外のどのディレクトリを使用してもかまいません（ルート ディレクトリでは GPG 暗号化が無効であるため）。

ルート ディレクトリの下にある場所を選択した場合は、ルート ディレクトリで GPG 暗号化を有効にする必要があります。

CLI を使用した Cisco Prime Collaboration Assurance データのバックアップ

CLI は SSH を介してのみサポートされます。telnet はサポートされません。Cisco Prime Collaboration サーバで使用されるポートは 26 です。リポジトリを作成した後、*admin* として Cisco Prime Collaboration サーバにログインし、次のコマンドを実行してデータをバックアップします。

```
admin# backup Backupfilename repository RepositoryName application cpcm
```

それぞれの説明は次のとおりです。

- *Backupfilename*：バックアップ ファイル名（拡張子 .tar.gpg なし）。この名前には最大 100 文字までの英数字を指定できます。
- *RepositoryName*：ファイルをバックアップする場所。この名前には最大 30 文字までの英数字を指定できます。

バックアップが完了すると、次のメッセージが表示されます。

```
% Creating backup with timestamped filename: Backupfilename-Timestamp.tar.gpg
```

バックアップ ファイルには、サフィックスとして末尾にタイム スタンプ（*YYMMDD-HHMM*）とファイル拡張子 .tar.gpg が付され、リポジトリに保存されます。

FTP サーバでのバックアップ例：

```
admin# backup assurance repository myftp application cpcm
```

ここで、myftp がリポジトリ名です。

バックアップ履歴の確認

バックアップ履歴を確認できます。Cisco Prime Collaboration Assurance サーバにログインします。

パス：[**システム管理（System Administration**）] > [**バックアップの設定（Backup Settings**）]

スケジュール済み、または設定済みのすべてのバックアップは、[バックアップの設定（Backup Settings）] ページにリストされます。[実行履歴（Run History）] 列から履歴を確認できます。詳細については、列にリストされている各ログのハイパーリンクをクリックしてください。

同じシステムでのデータの復元

以降の項では、同じシステムでデータを復元する処理について説明します。

データを復元するには、vSphere クライアントを使用して、VM コンソールから*admin*として Cisco Prime Collaboration アプリケーション サーバにログインします。SSH/Putty プロンプトから復元をトリガーすることを推奨しません。

Cisco Prime Collaboration データを復元するには、次のコマンドを実行します。

```
admin# restore Backupfilename repository RepositoryName application cpcm
```

ここで、*Backupfilename* は、サフィックスとして末尾にタイム スタンプ（*YYMMDD-HHMM*）とファイル拡張子 .tar.gpg が付いたバックアップ ファイルの名前です。

FTP サーバでの復元例：

```
admin# restore assurance_Sun_Feb_09_14_20_30_CST_2014.tar.gpg repository myftp application
cpcm
```

新しいシステムでの復元

Cisco Prime Collaboration では、システムのデータをバックアップし、システム全体に障害が発生した場合に別のシステムでデータを復元することができます。

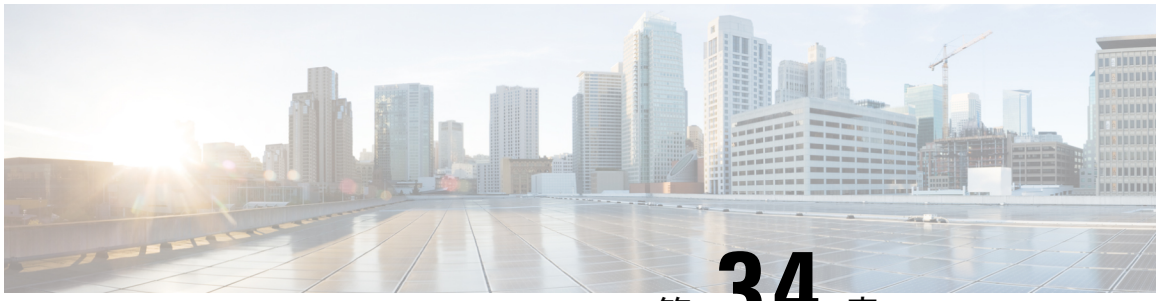
別のシステムからのバックアップを復元するには、次の手順を実行します。

データの復元先のシステムには、バックアップされたシステムと同じ MAC アドレスが必要です（IP アドレスとホスト名は違っていてもかまいません）。

システム（バックアップされた元のシステム）の MAC アドレスを別のシステムに割り当てることができない場合は、Cisco TAC に新しいライセンス ファイル（新しい MAC アドレス用）に関する情報をお問い合わせください。

別のシステムからのバックアップを復元するには、vSphere クライアントを使用して VM コンソールを介して管理者としてログインし、「データの復元」の説明に従って復元を実行します。「リポジトリの作成 」も参照してください。

Note 実行後の要件として、データの復元後にはすべてのデバイスを再検出する必要があります。



第 34 章

ログ レベルの設定

このセクションでは、次の点について説明します。

- ログ レベルの設定 （725 ページ）

ログ レベルの設定

この章では、Cisco Prime Collaboration Assurance でサポートされているさまざまなログ レベルに関する情報を提供します。

ログ レベル

Cisco Prime Collaboration Assurance は次のログ レベルをサポートしています。

- デバッグ - アプリケーションのデバッグに使用します。
- 情報：アプリケーションの進捗状況を示します。
- 警告：害を及ぼす可能性がある状況を示します。
- エラー：アプリケーションが引き続き実行可能であることを示します。
- 深刻：深刻なエラーを示します。このレベルは、すべてのモジュールでリストされるわけではありません。

ロギングを無効にすることはできません。ただし、次の作業を実行できます。

- 必要に応じて、ログ レベルを上げ、さらに多くのデータを収集する（最も高度なレベルは [Debug]）。
- デフォルト ログ レベル（[Error]）に戻す。

ログ レベルの設定は、[ログの管理（Log Management）] ページ（ の順に移動）から変更できます。**[システム管理（System Administration）] > [ログの管理（Log Management）]**。ログ ファイルはバックアップ ファイルにも含められます。

⚠

注意 ログ レベル設定を変更する場合は、必ず Cisco Technical Assistance Center（TAC）チームにお問い合わせください。

ログのダウンロード

この機能では、ログ ファイルのダウンロードを有効にして必要なログを共有できるようにして、ネットワークの問題を迅速に解決するための情報を提供します。

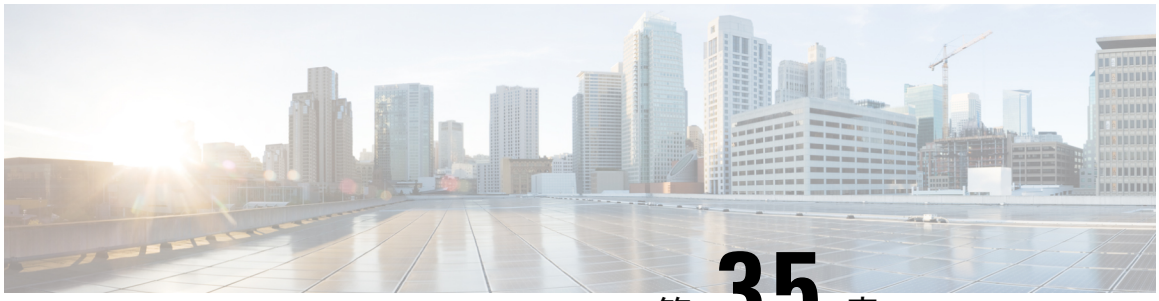
前提条件：ログを収集するモジュールで、ログ レベルを**デバッグ**に設定する必要があります。ログ レベルを [Debug] に設定する方法については、前述の項を参照してください。

ログをダウンロードするには **[ログのダウンロード（Download Log）]** ボタンをクリックします。.tar ファイルをダウンロードするよう要求されます。ファイル名は、（tar.）ファイルが生成された日時を示すため、ログファイル、日付、タイムスタンプ（Cisco Prime Collaboration Assurance のサーバ タイムに基づく）を生成したユーザのユーザ名を示します。ログ ファイルを表示するには、この同じ名前でファイルを開くか、または解凍します。ログファイルは圧縮ファイルで、7-Zip などの解凍ユーティリティで開くことができます。

第 X 部

Unified Communication Operations ダッシュボード

- Unified Communication Operations ダッシュボードの概要 （729 ページ）
- しきい値設定 （733 ページ）
- システム設定 （735 ページ）
- レスポンダ設定 （739 ページ）



第 35 章

Unified Communication Operations ダッシュボードの概要

この章では、次の内容について説明します。

• Unified Communication Operations ダッシュボード （729 ページ）

Unified Communication Operations ダッシュボード

この項の内容は次のとおりです。

Unified Communication Operations Dashboard の概要

Unified Communication Operations Dashboard（UCOD）は、複数の PCA ノードから統合されたすべてのクラスタ情報を収集します。最大 10 個のレスポンダをサポートしています。UCOD は、1 つの特定のマスター サーバに登録されているさまざまな PCA サーバから、重要なアラートなどのクラスタ情報を収集します。つまり、各 PCA は**レスポンダ**であり、**マスター**と呼ばれる 1 つのノードと通信します。

PCA ノードにマスターをインストールすると、同じ PCA ノードにレスポンダをインストールできる、またはインストールできない場合があります。マスターは、対応するマスターに登録された複数のレスポンダからのクラスタ情報を示します。

PCA へのレスポンダのインストール

PCA にレスポンダをインストールすると、[UC 運用ダッシュボード（UC Operations Dashboard）] メニューが表示されます。**マスター**と**レスポンダ**（オプション）を同じ PCA サーバにインストールすることも、**レスポンダ**のみを別の PCA ノードにインストールすることもできます。

[UC 運用ダッシュボード（UC Operations Dashboard）] タブをクリックし、次のサブメニューを探してください。

a) UCODランディング（UCOD Landing）ページ：マスターが正常に登録されなければ、ランディングページは表示されません。マスターが登録されていない場合は、それを伝えるエラー メッセージがユーザに表示されます。
b) レスポンダの設定（Responder Settings）ページ: マスターをレスポンダに登録します。

次のタスク

UC 運用ダッシュボードの起動 （730 ページ）

UC 運用ダッシュボードの起動

マスター IP アドレスを登録して、[UC Operations Dashboard] タブから UCOD ランディングページのサブメニューに移動します。

（注） マスター IP アドレスを登録していない場合、「UC Operations Dashboard のマスター IP アドレスが正しく登録されていません。マスターを [レスポンダ設定ページ（Responder Settings Page）] のレスポンダに登録してください」というエラー メッセージが表示されます。

マスター IP アドレスの登録

PCA にログインします。

[UC 運用ダッシュボード（UC Operations Dashboard）] に移動して、[レスポンダ設定（Responder Settings）] をクリックします。

[UCOD マスターノード（UCOD Master Node）] フィールドにマスター IP アドレスを入力します。

[有効化（Enable）]をオンにし、[適用（Apply）] をクリックします。

登録が完了したら、[レスポンダ設定（Responder Setting）]ページにアクセスして、マスターをレスポンダに登録します。

手順

- [UC運用ダッシュボード（UC Operations Dashboard）] タブをクリックすると、[UCODログイン（UCOD Login）] ページが表示されます。
- ユーザ名に **globaladmin**（小文字）と入力し、PCA のパスワードと同じパスワードを入力すると、UCOD のランディング ページが表示されます。
- ユーザ名には **globaladmin** 以外は入力できません。「ユーザ名またはパスワードが無効です。もう一度入力してください」というエラー メッセージが表示されます。

次のタスク

Unified Communication 運用ダッシュボードのランディング ページ

Unified Communication Operations のランディングページ

このページには、次のフィールドで示されたとおり、Unified Communication Manager クラスタの情報で構成されています。

フィールド	説明
UCM クラスタ	Cisco Unified CM クラスタの名前（VCS クラスタはサポートされていません）。
クリティカル アラート	指定したクラスタのクリティカル アラート数を表示します。
CPU 使用率（平均、ピーク）	指定したクラスタの一部であるすべてのノードの平均およびピークの CPU 使用率に基づき、CPU 使用率に関する情報を表示します。
仮想メモリ（平均、ピーク）	重大度を基にした、指定したクラスタの一部であるすべてのノードの家臣マシンの平均およびピークの使用率に基づき、仮想メモリに関する情報を表示します。
ディスク使用率（平均、ピーク）	指定したクラスタの一部であるすべてのノードの平均およびピークの ディスク使用率に基づき、ディスク使用率に関する情報を表示します。
コール（試行数 + 完了数）	指定したクラスタで、試行および完了したコール数を足した数を表示します。
未登録のエンドポイント（%、実際値）	指定したクラスタで登録されていないハードおよびソフトエンド ポイントの割合と、このクラスタ内で登録されていないエンドポイント数の実際値を足した数を表示します。値を示すシンボルは、重大度を表しています。
未登録のゲートウェイ（%、実際値）	指定したクラスタで登録されていない MGCP ゲートウェイ数の割合と、このクラスタ内で登録されていないエンドポイント数の実際値を表示します。値を示すシンボルは、重大度を表しています。
未登録のメディアリソース（%、実際値）	指定したクラスタで、登録されていないメディア リソース数の割合と、このクラスタ内で登録されていないエンドポイント数の実際値を表示します。値を示すシンボルは、重大度を表しています。

（注） CPU 使用率（平均、ピーク）、仮想メモリ（平均、ピーク）、ディスク使用率（平均、ピーク）には値に対して記号が付いており、これらの値は重要度に基づき並べ替えられています。

上記のすべてのフィールドには、値に対していくつかのシンボルが付けられており、これは**重大度**を表します。

これらのシンボルの上にマウスのカーソルを合わせると、それぞれの[しきい値の条件（Threshold Criteria）] を読み取ることもできます。

これらのホバー メッセージの内容は、しきい値設定 への変更に応じて適宜変更されます。

シンボルおよびホバー メッセージの説明は、次のとおりです。

記号

1. 赤いクロス - クリティカル
2. 黄色の三角形 - 警告
3. 緑色の丸チェック - 情報

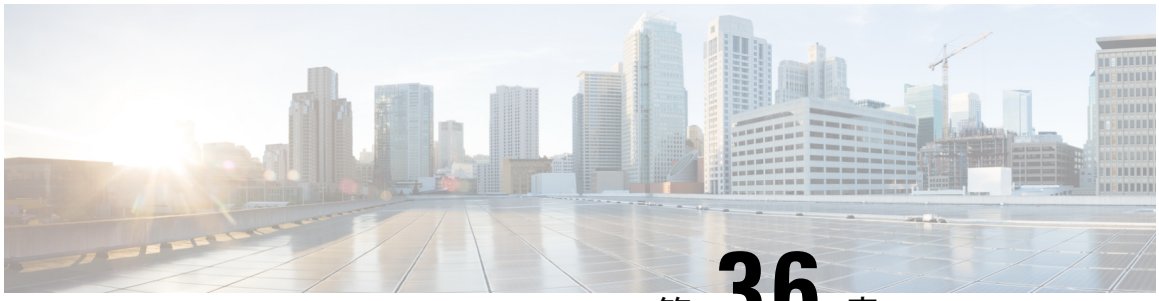
ホバー メッセージ

1. 0 ~ 50%（含む）のしきい値
2. 50 ~ 70%（含む）のしきい値
3. 70% を超えるしきい値

UCOD ランディングページの設定の下にあるサブメニューにアクセスする方法

下のサブメニューを表示するには、**UCOD ランディング**ページの右上隅にある **[設定（Settings）]** アイコンをクリックします。

1. しきい値設定
2. システム設定



第 36 章

しきい値設定

この章では、次の内容について説明します。

- しきい値設定の概要 （733 ページ）

しきい値設定の概要

[しきい値設定（Threshold Settings）]ページには、**CPU使用率、仮想メモリ、ディスク使用率、未登録のエンドポイント、未登録のゲートウェイ、未登録のメディアリソース**などのしきい値パラメータの条件が、パーセンテージで表示されます。

しきい値設定のテーブルには、デフォルト値が表示されます。デフォルト値を上書きするように選択し、重要なパラメータを定義することができます。ここで設定したデータは、ダッシュボードに反映されます。

しきい値設定

しきい値パラメータの重大度レベルを設定できます。

ステップ 1 デフォルトのしきい値パラメータ値を復元するには、テーブルの下にある [デフォルトにリセット（Reset to Default）] をクリックします。

ステップ 2 [保存（Save）]をクリックして、設定を保存します。

保存が正常に完了したら、ランディング ページに移動して、保存されているこれらのしきい値に基づいて、重大度が更新されたことを示すカラムを検索します。

無効なデータを入力すると [保存（Save）]

（注） ボタンは無効になり、関連するエラー メッセージが各フィールドに表示されます。エラー メッセージは、カラムごとに異なります。

しきい値パラメータ

しきい値パラメータには、次の 3 つの重大度レベルがあります。

1. 深刻
2. 警告
3. 情報

以下には、ルールが表示されています。無効なデータを入力すると、フィールドには重大度が表示されます。

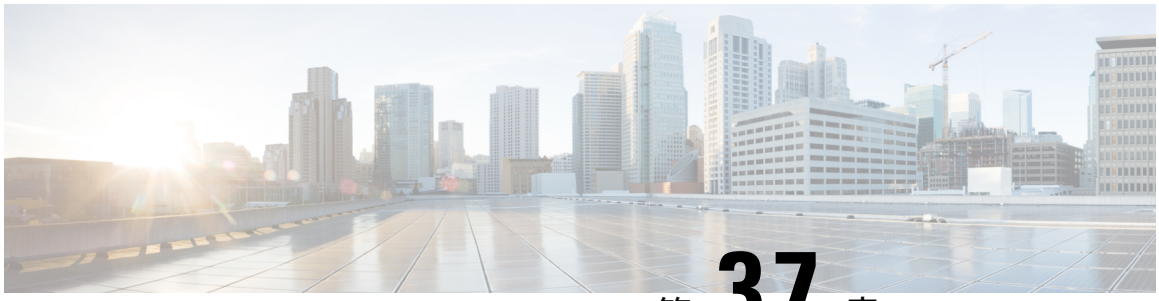
重大度	説明
深刻	[Critical Min] しきい値は、[Warning Max] しきい値以上となる必要があります。
情報	[Information Max] しきい値は、[Warning Min] しきい値以下となる必要があります。
Warning-Max しきい値	[Warning-Max] しきい値は、[Critical Max] しきい値以下、ならびに [Warning Min] しきい値以上となる必要があります。
Warning-Min しきい値	[Warning Min] しきい値は、[Min] しきい値以上、ならびに [Warning Max] しきい値以下となる必要があります。

表示には、デフォルトのしきい値条件が示されています。

基準	範囲
深刻	70% 以上および 100% 以下
警告	50% 以上および 70% 以下
情報	0% 以上および 50% 以下

（注） お互いが重複しない連続したカスタム範囲を指定する必要があります。たとえば、[Critical] 範囲が 80 ~ 100 で、[Warning] 範囲が 60 ~ 70 は有効ではありません。

1. **UCOD ランディング** ページの右上隅にある **[設定（Settings）]** をクリックします。
2. ドロップダウンリストから **[システム設定（System Settings）]** をクリックします。**[システム設定（System Settings）]** ページが表示されます。



第 37 章

システム設定

この章では、次の内容について説明します。

- システム設定 （735 ページ）

システム設定

[システム設定（System Settings）] ページで、マスター アプリケーションを設定します。このページで、監視するレスポンダ（PCA ノード）を追加できます。

- [はい（Yes）] をクリックすると、マスターノードが有効になります。
- [いいえ（No）] をクリックすると、マスター ノードが無効になります。「UC運用ダッシュボードのマスターノードを無効にしますか」というメッセージが表示されます。
- [はい（YES）] をクリックして、マスターノードの削除を確認します。

（注） マスターの有効化は、デフォルトで [はい（Yes）] の状態にあります。マスターを無効にすると、マスターとそれに関連付けられたレスポンダとの間で通信は行われません。

関連付けられたレスポンダの追加または削除

表には、関連付けられているレスポンダの一覧が示されています。

フィールド	説明
ホスト名	レスポンダノードのホスト名です。
IP アドレス	レスポンダノードの IP アドレスです。
管理されたクラスタ数	関連付けられたレスポンダノードで管理されているクラスタの数です。

フィールド	説明
レスポンダ ステータス	Master に登録したレスポンダのステータスを表示します。
登録日時	レスポンダを Master に登録、または登録解除された日時です。
ステータス理由	Master に登録した各レスポンダのステータスに関する理由を示します。さまざま理由が、次のとおりに表示されます。 **1.** 登録の却下 **理由** - マスター IP がレスポンダ側で承認されていません **2.** 正常に登録されました **3.** レスポンダが Suspended モードです **4.** レスポンダに連絡できません **5.** レスポンダが登録解除を開始しました **6.** 過去 2 サイクルの間にデータを受信していません

関連付けられたレスポンダの追加または削除

1. **[追加（Add）]** をクリックして、関連付けられたレスポンダを追加します。

   ポップアップした **[レスポンダ IP（Responder IP）]** フィールドに、追加するコンマ区切りのマスター IP アドレスまたはホスト名を入力します。

2. 削除するレスポンダのボックスをオンにします。

   [選択したレスポンダを削除しますか（Do you want to delete the selected Responder(s)）] というメッセージが表示されます。

   選択したレスポンダを削除するには、**[はい（Yes）]** をクリックします。

   選択したレスポンダを維持するには、**[いいえ（No）]** をクリックします。

（注） **[システム設定（System Settings）]** ページでレスポンダを削除すると、対応するクラスタ データも削除されます。

ジョブ頻度の設定

[Cluster Summary Job Frequency] のドロップダウン ボックスを使用し、必要に応じてクラスタ概要のジョブ頻度を 1、3、5、または 10 分に設定します。

（注） デフォルトの時間間隔は **5** 分です。

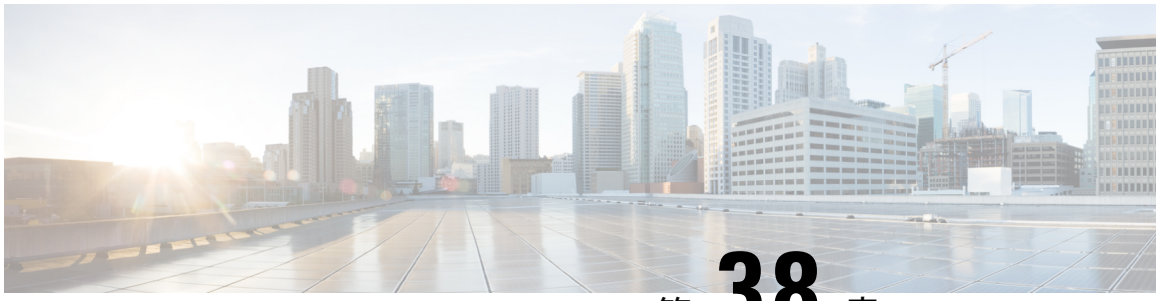
[適用（Apply）] をクリックします。

（注）
1. ジョブ頻度は、すべてのレスポンダに適用されます。選択した各時間間隔に対して、レスポンダは、集計されたクラス概要に関する情報を Master に送信します。
2. メガク ラスタの場合、間隔が大きければ大きいほど（> 5分）精度が高まります。小さいクラスタ（ノード数が -3 ~ 5）と少ない PCA（<= 5）の場合は頻度を少なくします。

共有秘密キーの設定

手順

- マスターの設定中に [レスポンダ設定（Responder settings）] ページで設定したのと同じ共有秘密キーを入力します。
- Master と関連付けられたレスポンダの両方に同じキーを提供する必要があります。
- [システム設定（System Settings）] ページですべてのフィールドを設定したら、[適用（Apply）] をクリックします。



第 38 章

レスポンダ設定

この章では、次の内容について説明します。

- レスポンダ設定の概要 （739 ページ）

レスポンダ設定の概要

このページには、**[レスポンダ設定（Responder Settings）]** の完全な情報があります。

レスポンダをインストールすると、デフォルトでは **[Suspend]** 状態になります。つまり、レスポンダがデータを収集または送信することはありません。この状態では、マスター IP アドレスと共有秘密鍵はデフォルトで **[Disable]**状態になってい ます。

レスポンダの有効化

ステップ 1 [有効化（Enable）] をクリックし、[レスポンダの設定（Responder Settings）] ページで、レスポンダの状態を手動で選択します。

ステップ 2 [UCOD マスターノード（UCOD Master Node）] フィールドに、ホスト名またはマスター IP アドレスのいずれかを入力します。

共有秘密キーの設定

レスポンダの状態を有効にして UCOD マスターノードを入力し、**共有秘密鍵**を設定します。これは任意ですが、データを保護するため強く推奨します。これは Master とレスポンダ間の通信を保護します。

（注） Master と関連付けられたレスポンダの両方に同じキーを提供する必要があります。

共有秘密鍵は、以下のポリシーに基づき設定します。

鍵のポリシー：

1. 英数字（大文字と小文字を区別）
2. 長さは 8 ～ 24 文字
3. 特殊文字は不可

登録ステータス

ステップ 1 [適用（Apply）] をクリックして、レスポンダの設定を正常に登録します。

共有秘密キーを設定すると、それに応じて登録ステータスが変更されます。

ステップ 2 以下のそれぞれの理由を確認してください。

1. **登録済み**：マスターへの登録が正常に終了した。
2. **保留中**：レスポンダが中断されているか、またはマスターが登録に利用できない（デフォルトの状態）。
3. **未登録**：レスポンダの IP がマスターの承認済みリストにない。
4. **一時停止**：レスポンダが中断状態である。ただし、マスターは、承認済みリストにこのレスポンダ IP を持っている。

   マスターIPアドレス/共有秘密キーの検証が正常に行われると、レスポンダは正常にマスターに登録されます。

   （注） 正しいマスター IP アドレスやホスト名を指定しない場合、[レスポンダ設定（Responder Settings）] ページの [適用（Apply）] ボタンは無効になります。

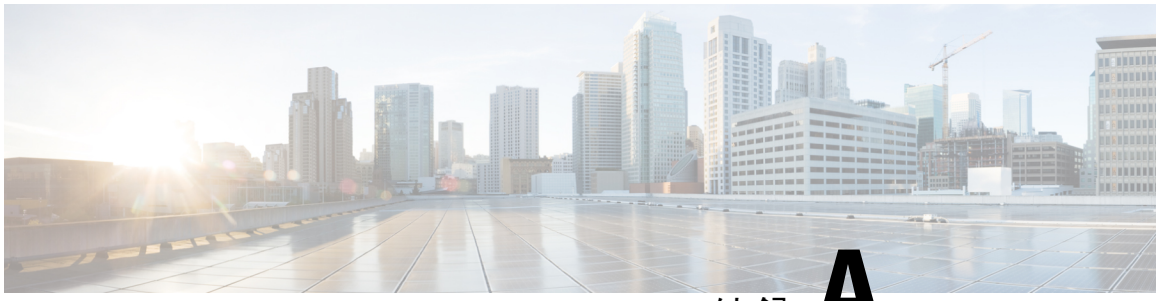
付 録

参考資料

このセクションでは、Synthetic Test Worksheet、Cisco 1040 Sensor Management、ユーザ インターフェイスに関する情報を提供します。

- Synthetic Test ワークシート （743 ページ）
- Cisco 1040 センサー管理 （747 ページ）
- セキュアな JTAPI 接続のトラブルシューティング （759 ページ）
- Jetty および Tomcat サーバの TLS 設定 （761 ページ）
- ユーザ インターフェイス （765 ページ）

参考資料



付録 A

Synthetic Test ワークシート

このセクションでは、次の点について説明します。

- Synthetic Test ワークシート （743 ページ）

Synthetic Test ワークシート

模擬テストで使用するために Cisco Unified Communications Manager 内で作成する必要がある電話機の数は、次のものによって決まります。

- 設定する模擬テストの数。
- 実行するテストのタイプ。

次の表は、必要な電話機の数を決定するためのワークシートです。表に記載されている情報を使用して、テストの回数を入力し、必要な電話機の総数を計算してください。

表 *100*：模擬テストで必要となる電話数

テストの回数	テストのタイプ	テストに必要な電話の数	必要となる合計の電話数
	Phone Registration	1（模擬電話）	
	Dial-Tone	1（模擬電話）	
	実際の電話を使用した End-to-End Call	2（模擬電話 1 および実際の電話 1）	
	模擬電話を使用した End-to-End Call	2（模擬電話）	
	TFTP Download	0	
	Cisco Prime Collaboration リリース 11.6 以降の場合 HTTP ダウンロード	0	

テストの回数	テストのタイプ	テストに必要な電話の数	必要となる合計の電話数
	Emergency Call（On Site Alert Number なし）	2（模擬電話）	
	Emergency Call（On Site Alert Number あり）	3（模擬電話）	
	Message-Waiting Indicator	2（模擬電話）	

各 Unified CM の電話機を設定する際は、次のワークシートを使用すると Cisco Prime Collaboration Assurance へのデータ入力が簡単になります。

表のダッシュは、MAC アドレス、宛先の電話の内線番号、または宛先の電話の Cisco Unified Communications Manager にデータが必要とされないことを示します。

表 *101 : Cisco Unified Communications Manager*

Synthetic Test	**MAC アドレス**	**宛先の電話の内線番号**	**宛先の電話の Cisco Unified Communications Manager**
電話登録		-	-
ダイヤルトーン		-	-
エンドツーエンド コールの発信元電話機		-	-
エンドツーエンド コールの接続先電話機（模擬電話機）			
エンドツーエンド コールの接続先電話機（実際の電話機）	-		-
電話登録		-	-
ダイヤルトーン		-	-
エンドツーエンド コールの発信元電話機		-	-
エンドツーエンド コールの接続先電話機（模擬電話機）			
エンドツーエンド コールの接続先電話機（実際の電話機）	-		-
電話登録		-	-
ダイヤルトーン		-	-

エンドツーエンド コールの発信元電話機		-	-
エンドツーエンド コールの接続先電話機（模擬電話機）			
エンドツーエンド コールの接続先電話機（実際の電話機）	-		-

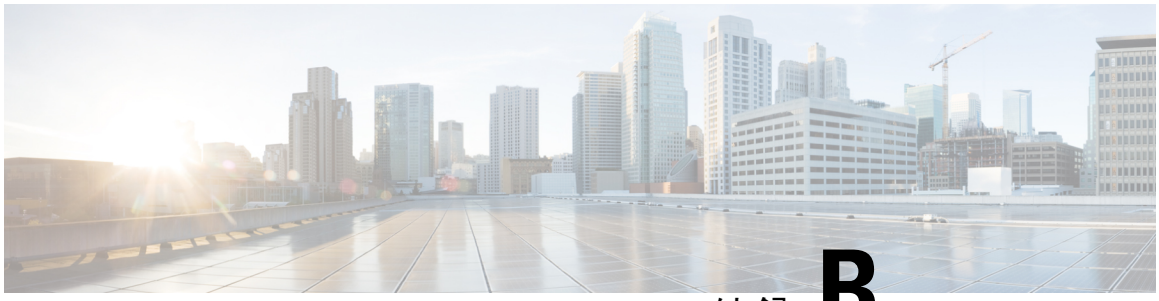
表 *102 : Cisco Emergency Responder*

パラメータ	名前または番号
送信元	
Cisco Unified Communications Manager	
MAC アドレス	
送信先	
緊急番号	
Public Safety Answering Point	
Cisco Unified Communications Manager	
MAC アドレス	
On Site Alert	
Cisco Unified Communications Manager	
MAC アドレス	

表 *103 : Cisco Unity*

パラメータ	名前または番号
発信者	
Cisco Unified Communications Manager	
MAC アドレス	
受信者	
Cisco Unified Communications Manager	
MAC アドレス	
電話の内線番号	

ボイスメール	
パスワード	



付録 B

Cisco 1040 センサー管理

このセクションでは、次の点について説明します。

• Cisco 1040 センサー管理 （747 ページ）

Cisco 1040 センサー管理

Cisco Prime Collaboration Assurance は 、Cisco 1040 センサーから受信したデータを使用してネットワーク内の音声伝送の品質を判断します。

を必要に応じて動作するには 、Cisco 1040 に接続するスイッチを管理し 、Cisco Prime Collaboration Assurance で設定する必要があります。詳細については、『Cisco Prime Collaboration Assurance and Analytics インストールおよびアップグレード ガイド』を参照してください。

（注） Cisco 1040 センサーの管理は、Cisco Prime Collaboration Assurance を MSP モードでインストールした場合には適用されません。

この項の内容は、次のとおりです。

Cisco Prime NAM/vNAM の概要

Cisco 1040 センサーの販売は終了いたしました。詳細については、「Cisco 1040 センサーの販売および生産終了」ページを参照してください。

Cisco 1040 センサーは Cisco Prime NAM/vNAMCisco に置き換えられ、不足する機能を満たします。Cisco Prime Network Analysis Module（NAM）と Cisco Prime Collaboration Assurance を同時に使用して、音声やその他のネットワークに関連する問題を監視し、トラブルシューティングを行うことができます。詳細については、Using Cisco Prime Virtual Network Analysis Module および Cisco Prime Collaboration を使用して音声とビデオを監視およびトラブルシュート」のホワイトペーパーを参照してください。

NAM レポートから取得できる情報については、NAM & Sensor Report （510 ページ）を参照してください。

Cisco Prime Collaboration Assurance の初期設定を実行

Cisco 1040 センサーの初期設定を行うには、次の手順を実行します。

ステップ 1 Cisco Prime Collaboration Assurance と Cisco 1040 センサーを使用するには、1 台以上の TFTP サーバを追加します。「Cisco 1040 設定およびイメージ ファイル用の TFTP サーバの設定」を参照してください。

ステップ 2 デフォルトのコンフィギュレーション ファイルを作成します。「Cisco 1040 センサー デフォルト設定のセットアップ」を参照してください。

Cisco 1040 がネットワークに接続されるときは、Cisco Prime Collaboration Assurance に登録される前に、TFTP サーバから設定ファイルがダウンロードされます。

Cisco 1040 設定およびイメージ ファイル用の TFTP サーバの設定

Cisco Prime Collaboration Assurance では、Cisco 1040 用の設定ファイルとバイナリ イメージ ファイルを提供するために、1 つ以上の TFTP サーバが使用されます。Cisco Prime Collaboration Assurance で使用する TFTP サーバを少なくとも 1 つ定義する必要があります。バックアップ サーバが必要な場合や、複数の DHCP スコープがある場合は、追加の TFTP サーバを設定することができます。

TFTP サーバで書き込みの失敗が発生した場合は、Cisco Prime Collaboration Assurance がサーバ上に保持している設定ファイルを使用して復旧できます。この場合、Cisco Prime Collaboration Assurance 用に設定されている各 TFTP サーバに、Cisco Prime Collaboration Assurance から手動で設定ファイルをコピーします。

TFTP サーバの追加と削除

Cisco Prime Collaboration Assurance への Cisco 1040 の登録を可能にするには、Cisco Prime Collaboration Assurance が Cisco 1040 の設定ファイル（およびバイナリ イメージ ファイル）を提供できるように、少なくとも 1 つの TFTP サーバを定義する必要があります。

（注）

- Cisco Prime Collaboration Assurance を TFTP サーバとして使用することはサポートされていません。また、Cisco Prime Collaboration Assurance サーバで CWCS TFTP サービスを無効にすることを推奨しています。
- Unified CM を TFTP サーバとして使用する場合は、
  - 設定ファイルとイメージ ファイルを Cisco Prime Collaboration Assurance から Unified CM TFTP サーバのルートロケーションに手動でコピーする必要があります。
  - ファイルを更新して TFTP サーバにコピーした後、Cisco 1040 がそのファイルをダウンロードできるよう、（Unified CM 上の）Cisco TFTP サービスを再起動することが必要になる場合もあります。

ステップ 1 選択 **[アラームおよびレポート管理（Alarm & Report Administration）] > [1040 センサーのセットアップ（1040 Sensor Setup）] > [TFTP サーバ（TFTP Servers）]**。
TFTP サーバ セットアップ ページが表示されます。

ステップ 2 [Add] をクリックします。
[TFTP サーバの設定（TFTP Server Setting）] ダイアログボックスが表示されます。

ステップ 3 次のフィールドにデータを入力します。

- TFTP サーバ：IPアドレスまたは DNS 名
- ポート番号：慣例的なポート番号は 69 です。

ステップ 4 **[OK]**をクリックします。

（注） 削除するには、TFTP サーバを選択して [削除（Delete）] をクリックします。

Cisco 1040 センサー デフォルト設定のセットアップ

この手順は、次の目的で使用します。

- コール メトリックのアーカイブの有効化または無効化：Cisco Prime Collaboration Assurance によって、MOS データがデータベースに保存されます。このデータをファイルにも保存することができます。
- アーカイブ データ ファイルおよび Cisco 1040 イメージ ファイルのディレクトリ パスを表示します。
- デフォルト設定ファイルの作成：QOVDefault.CNF は、Cisco 1040 が登録可能なプライマリ Cisco Prime Collaboration Assurance を指定します。

（注） Unified CM ソフトウェア バージョン 4.2 以降のバージョンを TFTP サーバとして使用している場合は、Cisco Prime Collaboration Assurance サーバの画像ファイル ディレクトリから Unified CM TFTP サーバ上のルートの場所にデフォルト設定ファイルを手動でコピーする必要があります。詳細については、次の手順のステップ 3 を参照してください。

Cisco 1040 センサーを設定するには、次の手順を実行します。

ステップ 1 選択（Select） **[アラームおよびレポートの管理（Alarm & Report Administration）] > [1040 センサー（1040 Sensors）]**
[セットアップ（Setup）] ページが表示されます。

ステップ 2 次の表に説明されているデータをアップデートします。

ステップ 3 **[OK]**をクリックします。Cisco Prime Collaboration Assurance によって、設定ファイルがローカルに保存され、Cisco Prime Collaboration Assurance に追加された TFTP サーバにコピーされます。

Cisco 1040 センサー/NAM セットアップ ページ：グラフィカル ユーザ インターフェイス要素

表 *104 : Cisco 1040* センサー*/NAM* セットアップ ページ：グラフィカル ユーザ インターフェイス要素

グラフィカルユーザインターフェイスの要素	説明
コール メトリックのアーカイブ	次のいずれかを選択します。 • [有効（Enable）]：分析後、Cisco Prime Collaboration Assurance により、センサーからディスク ファイルにデータが保存されます。 • [無効化（Disable）]：分析後に、Cisco Prime Collaboration Assurance がデータを破棄します。 デフォルト：Disable。
データ ファイル ディレクトリ	コール メトリックのアーカイブがイネーブルになっている場合に、ファイルが保存されるディレクトリ。このフィールドは編集できません。
画像ファイル ディレクトリ	Cisco 1040 バイナリ イメージ ファイルと設定ファイルがローカルに保存されているディレクトリ。このフィールドは編集できません。
抑制エンドポイントごとに *n* 分ごとにトラップを送信します。	5 以上の数値を入力します。Cisco 1040s は、60 秒ごとに Cisco Prime Collaboration Assurance にデータを送信します。Cisco Prime Collaboration Assurance は、しきい値を超えたかどうかをエンドポイントごとに判断し、状況に応じて 1 分間隔でトラップを送信できるようになっています。この設定を使用すると、Cisco Prime Collaboration Assurance が各エンドポイントに送信するトラップ数を減らすことができます。1つのエンドポイントに対して、トラップは *n* 分ごとに送信され、その間追加トラップは抑制されます（送信されない）。
TFTP サーバに対するデフォルト設定	

グラフィカルユーザインターフェイスの要素	説明
画像ファイル名	新しいイメージを使用している場合は、イメージ ファイル名を入力します（製品のアップグレード後など）。
プライマリ Prime Collaboration	プライマリ Cisco Prime Collaboration Assurance の IP アドレスまたは DNS 名。

Cisco Prime Collaboration Assurance で Cisco 1040 センサーを設定

Cisco Prime Collaboration Assurance は、音声ネットワークにインストールされている Cisco 1040 センサーから受信したデータを分析します。Cisco Prime Collaboration Assurance は複数の Cisco 1040 センサーを管理します。

この項の内容は、次のとおりです。

Cisco 1040 センサーの詳細

Cisco 1040 センサーの詳細を表示するには、**[アラームおよびレポートの管理（Alarm & Report Administration）]** > **[1040センサーのセットアップ（1040 Sensor Setup）]** > **[管理（Management）]**。[Cisco 1040センサーの詳細（Cisco 1040 Sensor Details）] ページに、次の表に示す情報が表示されます。

グラフィカルユーザインターフェイスの要素	説明
	[Cisco 1040センサー/NAMの詳細（Cisco 1040 Sensor/NAM Details）] ページのデータを CSV または PDF ファイルにエクスポートします。
	データを印刷に適した形式で別のウィンドウに表示します。ブラウザ ウィンドウから印刷する場合に使用します。
[Check Box] カラム	編集、リセット、または削除する Cisco 1040 を選択します。
[Name] カラム	名前のリンクをクリックすると、その Cisco 1040 の設定の詳細が表示されます。
[Cisco 1040 Address] カラム	Cisco 1040 の MAC アドレスと IP アドレスが表示されます。MAC アドレスのリンクをクリックすると、その Cisco 1040 に関する HTML ページが起動されます。

グラフィカルユーザインターフェイスの要素	説明

[Prime Collaboration] カラム	次のステータスが表示されます。
	• [プライマリ（Primary）]：Cisco 1040 に対して定義されているプライマリ Cisco Prime Collaboration Assurance の IP アドレスまたはホスト名。
	• [登録先（Registered with）]：次のいずれかが表示されます。
	  • Cisco 1040 が現在データを送信している Cisco Prime Collaboration Assurance の IP アドレスまたはホスト名。
	  • [待機中（Waiting）]：Cisco 1040 はまだ登録されていません。
	  • [古いイメージ（Older Image）]：Cisco 1040 上のバイナリ イメージはサポートされていません。

時間のリセット列	Cisco Prime Collaboration Assurance が最後に Cisco 1040 にリセット コマンドを送信した日付と時刻。
ボタン	
追加	「Cisco 1040 センサーの追加」を参照してください。
編集	「複数の Cisco 1040 設定を編集」を参照してください。
削除	「Cisco 1040 センサーの削除」を参照してください。
リセット	「Cisco 1040 のリセット」を参照してください。
更新	[Cisco 1040 Sensor Details] ページを更新します。

プロセスの再起動による Cisco Prime Collaboration Assurance の Cisco 1040 登録情報の更新

Cisco Prime Collaboration Assurance で、Cisco 1040 センサーから syslog を受信して処理しているにもかかわらず、センサーが登録待機中として表示される場合があります。この問題は、ユーザが次のいずれかの操作を行った後に発生することがあります。

- **pdterm** を使用して QOVR プロセスを停止し、すぐに **pdexec** を使用して QOVR プロセスを再起動した。この問題を防ぐには、QOVR プロセスの停止と再起動の間隔を 5 分以上あけます。この問題を解決するには、次の手順を実行します。

  コマンドラインから次のコマンドを入力して、QOVR プロセスを再び停止します。

  ```
  pdterm QOVR
  ```

  5 分以上待ちます。

  次のコマンドを入力します。

  ```
  Pd 3QVR(pd 3/3QVR
  ```

- Cisco Prime Collaboration Assurance がインストールされているシステムの時刻を変更したが、その後でデーモンマネージャの停止と再起動を行わなかった。この問題を修正するには、admin としてログインし、次のコマンドを実行します。

  ```
  <hostname>/admin#application stop cpcm <hostname>/admin#application start cpcm
  ```

Cisco 1040 センサーの追加

Cisco 1040 センサーを Cisco Prime Collaboration Assurance に追加するには、次の手順を実行します。

ステップ 1 選択（Select）**[アラームおよびレポートの管理（Alarm & Report Administration）]** > **[1040センサーのセットアップ（1040 Sensor Setup）]** > **[管理（Management）]**。
[Cisco 1040センサー/NAMの詳細（Cisco 1040 Sensor/NAM Details）] ページが表示されます。

ステップ 2 [Add] をクリックします。
[Cisco 1040センサーの追加（Add a Cisco 1040 Sensor）] ダイアログ ボックスが表示されます。

ステップ 3 下の表にリストされているデータを入力します。

ステップ 4 **[OK]**をクリックします。設定ファイルが、Cisco Prime Collaboration Assurance がインストールされているサーバと、すべての TFTP サーバに保存されます。（「Cisco 1040 設定およびイメージ ファイル用の TFTP サーバの設定」を参照してください）。設定ファイルには、QOV<*MAC address*>.CNF のように名前が付けられます。<*MAC address*> は Cisco 1040 の MAC アドレスです。同様に、設定を更新する場合は、1 つまたは複数のチェックボックスをオンにし、[編集（Edit）] をクリックします。

（注）

- 名前または説明を編集するには、Cisco 1040 センサーを選択します。
- Cisco 1040 のコンフィギュレーション ファイルは、テキスト エディタを使用して編集しないでください。

Cisco 1040 センサー/NAM ダイアログ ボックス：グラフィカル ユーザ インターフェイス要素の説明

グラフィカルユーザインターフェイスの要素	説明
センサー名	20文字以内で入力します。この名前は、レポートなど、Cisco Prime Collaboration Assurance ウィンドウのセンサーを識別するために使用されます。 （注） Cisco 1040 の名前は一意でなければなりません。デフォルト設定ファイルを使用して Cisco Prime Collaboration Assurance に登録する Cisco 1040 には、Cisco 1040 + <*MAC* アドレスの末尾 *6* 桁> という名前を使用します。
画像ファイル名	バイナリ イメージ ファイル名を入力します。ファイル名の形式は SvcMonAB2_*nnn*.img です。*nnn* はリビジョン番号です。
MAC アドレス	追加する Cisco 1040 の MAC アドレスを入力します。
プライマリ Prime Collaboration	Cisco Prime Collaboration Assurance がインストールされているホストの IP アドレスまたは DNS 名を入力します。
説明	（任意）最大 80 文字を入力します。

複数の Cisco 1040 設定を編集

- TFTP サーバとして Unified CM を使用している場合は、更新された設定ファイルを Cisco Prime Collaboration Assurance サーバの画像ファイル ディレクトリから Unified CM TFTP サーバ上のルートの場所に手動でアップロードする必要があります。その後で、Cisco 1040 をリセットする必要があります。（イメージファイルのディレクトリは *NMSROOT*/ImageDir です。*NMSROOT* は、Cisco Prime Collaboration Assurance がインストールされるディレクトリです。デフォルトの場所は「C:\Program Files\CSCOpx」）Cisco 1040 で最新ファイルが登録されない、または読み込まれない場合は、TFTP サーバを再起動してください。
- Cisco 1040 のコンフィギュレーション ファイルは、テキスト エディタを使用して編集しないでください。Cisco 1040 のコンフィギュレーション ファイルを編集するときは、必ずここで説明する手順を使用してください。

複数の Cisco 1040 の設定を編集するには、次の手順を実行します。

ステップ 1 選択（Select）**[アラームおよびレポートの管理（Alarm & Report Administration）]** > **[1040センサーのセットアップ（1040 Sensor Setup）]** > **[管理（Management）]**。

ステップ 2 Cisco 1040 のチェックボックスを 1 つ以上オンにして、[編集（Edit）] をクリックします。

ステップ 3 任意のフィールドを更新します。

ステップ 4 **[OK]**をクリックします。
Cisco Prime Collaboration Assurance では、設定ファイルがローカルサーバに保存され、すべての TFTP サーバにコピーされます。次に、Cisco Prime Collaboration Assurance が複数の Cisco 1040 をリセットして、更新された設定を読み込むようにします。

Cisco 1040 管理：フィールドの説明

表 *105 : Cisco 1040* 管理：フィールドの説明

フィールド	
画像ファイル名	バイナリイメージファイル名を入力します。ファイル名の形式は SvcMonAB2_*nnn*.img です。*nnn* はリビジョン番号です。サポートされている最新のバイナリイメージファイルの名前については、『Cisco Prime Unified Service Monitor 2.3 互換性マトリクス』を参照してください。
プライマリ Prime Collaboration	Cisco Prime Collaboration Assurance がインストールされているホストの IP アドレスまたは DNS 名を入力します。Cisco 1040 は、この Cisco Prime Collaboration Assurance に到達不能になるまでデータを送信します。
セカンダリ Prime Collaboration	（任意）Cisco Prime Collaboration Assurance がインストールされているホストの IP アドレスまたは DNS 名を入力します。Cisco 1040 は、プライマリの Cisco Prime Collaboration Assurance が到達不能になった場合にのみ、この Cisco Prime Collaboration Assurance にデータを送信します。

Cisco 1040 のリセット

1 つ以上の Cisco 1040 をブートするには、次の手順を実行します。ブートされた Cisco 1040 は、初めに DHCP を使用して TFTP サーバの IP アドレスを取得します。Cisco 1040 は、TFTP サーバから設定ファイルを取得します。設定ファイルで、現在インストールされているイメー

ジと異なるバイナリ イメージ ファイルが指定されている場合、Cisco 1040 は、TFTP サーバからバイナリ イメージ ファイルを取得します。

ステップ 1 選択（Select）**[アラームおよびレポートの管理（Alarm & Report Administration）]** > **[1040センサーのセットアップ（1040 Sensor Setup）]** > **[管理（Management）]**。

ステップ 2 リセットする Cisco 1040 のチェックボックスを選択します。

ステップ 3 [リセット（Reset）] をクリックします。Cisco 1040 は、スタートアップ シーケンスが完了し、必要に応じて再設定を行い、Cisco Prime Collaboration Assurance に登録するのに数分かかります。

（注） Unified CM を TFTP サーバとして使用した場合、Cisco 1040 センサーはリセット後に、最新のイメージ ファイルの登録または読み込みが行われません。Cisco Prime Unified Communications Manager 上で、TFTP サービスを再起動する必要があります。

Cisco 1040 をリセットすると、Cisco Prime Collaboration Assurance によってセンサーに最新の時間が送信されます。Cisco 1040 は、自身のクロックを必要に応じて再設定します。

Cisco 1040 センサーの削除

Cisco Prime Collaboration Assurance から Cisco 1040 センサーを削除する前に、Cisco 1040 の 10/100-1 ファスト イーサネット ポートに物理的に接続されているスイッチ ポートを閉じる必要があります。

ステップ 1 このポートを特定するために、スイッチの IP アドレスとスイッチ ポートを Cisco 1040 の Web インターフェイスで調べます。

ステップ 2 ポートをシャットダウンするには、スイッチの CLI を使用します。

（注） スイッチ ポートを閉じる前に、Cisco Prime Collaboration Assurance から Cisco 1040 を削除しないようにしてください。

また、スイッチの SPAN または RSPAN 宛先ポートのシャットダウンまたは再設定も必要です。Cisco Catalyst スイッチおよびモジュールの SPAN および RSPAN の設定の詳細については、http://www.cisco.com/en/US/products/hw/switches/ps708/products_tech_note09186a008015c612.shtml を参照してください。

Cisco 1040 を削除した後、削除された Cisco Prime Collaboration Assurance に自動的に登録されません。削除された Cisco 1040 を Cisco Prime Collaboration Assurance に再登録するには、手動で Cisco 1040 センサーを追加する必要があります。「Cisco 1040 センサーの追加」を参照してください。

削除するには、**[アラームおよびレポートの管理（Alarm & Report Administration）]** > **[1040 センサーのセットアップ（1040 Sensor Setup）]** > **[管理（Management）]**。[Cisco 1040 センサーの詳細（Cisco 1040 Sensor Details）] ページから削除する Cisco 1040 のチェックボックス（複数可）をオンにし、[削除（Delete）] をクリックします。

（注） Cisco 1040 センサーを削除する前に、任意のセンサーしきい値グループから Cisco 1040 センサーを削除します。

Cisco Prime Collaboration Assurance から、時刻同期メッセージが各 Cisco 1040 センサーに1時間ごとに送信されます。Cisco 1040 登録時にも Cisco Prime Collaboration Assurance から時刻同期メッセージが送信されます。Cisco 1040 の登録が行われるのは、Cisco 1040 がネットワークに追加されたときと、リセットされたときです。Cisco Prime Collaboration Assurance から受信した時間で、Cisco 1040 は必要に応じてクロックをリセットします。

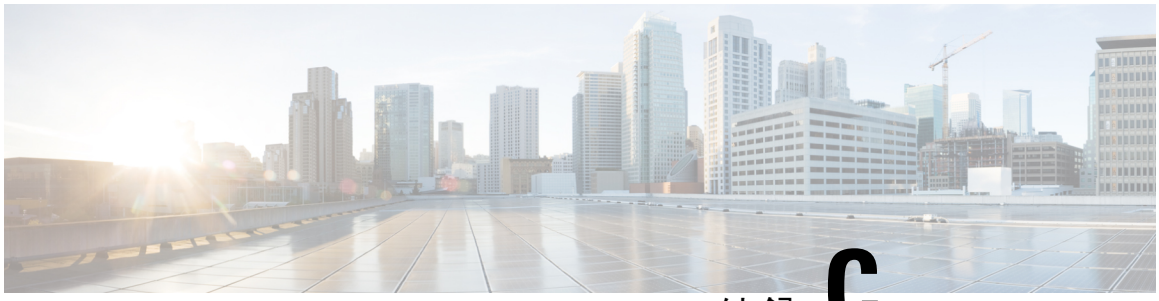
Cisco 1040 の診断情報を表示

Cisco 1040 に保存されている診断情報を表示するには、ブラウザに http://<*IP address*>/Diagnostics と入力します（IP アドレスは Cisco 1040 のアドレス）。

Cisco 1040 の Web インターフェイスに、[Diagnostics Information] ウィンドウが表示されます。表示される情報は次のとおりです。

フィールド	説明
Current Time	現在の日時（HH:MM:SS MM/DD/YYYY）です。
Clock Drift	秒数のずれとクロックがリセットされた前回の日時です。たとえば、「1 second(s) updated at 9:23:37 03/16/2009」です。
Last Analysis Time	Cisco 1040 が最後に分析を実行した日時です。
Streams Analyzed	最後のインターバル中に分析された RTP ストリームの数です。
Last Communication	センサーが ACK または timeSet メッセージを最後に受け取った日時、または Cisco Prime Collaboration Assurance からのサポートされているメッセージです。
Last Successful Report Time	Cisco 1040 が Cisco Prime Collaboration Assurance にデータを最後に送信した日時です。
Report Destination	レポートの送信先のホスト名または IP アドレスとポート番号。
Report Length (bytes)	最後のレポート レコードのバイト数。
Received Packets	Cisco 1040 が最後のインターバル中に受信したパケットの数。
Receive Errors	モニタリング インターフェイス上で受信されたエラーの数（pcap によって報告されたとおり）。

フィールド	説明
Packets Dropped	モニタリング インターフェイス上でドロップされたエラーの数（pcap によって報告されたとおり）。
Buffer overruns	モニタリング インターフェイス上のバッファオーバーランの数（pcap によって報告されたとおり）。
Framing Errors	モニタリング インターフェイス上のフレーム同期エラーの数（pcap によって報告されたとおり）。
Interface Promiscuous	モニタリング インターフェイスが無差別モード（yes）かそうでない（no）かを示します。



付録 C

セキュアな JTAPI 接続のトラブルシューティング

このセクションには、潜在的なエラーと、セキュアなJTAPI接続をトラブルシュートするための推奨アクションが一覧表示されています。

• セキュアな JTAPI 接続のトラブルシューティング （759 ページ）

セキュアな JTAPI 接続のトラブルシューティング

1. [Secure JTAPI] 用の CUCM セットアップでエラーが発生した可能性があります。
   1. [Secure JTAPI] 接続が動作するよう、CUCM を [Mixed] モードに移行させます。
   2. CUCM のアプリケーション ユーザには、「Standard CTI Secure Connection」 ロールが関連付けられていません。

（注） セキュリティで保護されていない接続では、「Standard CTI Secure Connection」 ロールが表示されることはありません。

   3. アプリケーションユーザCAPFプロファイルには、「インストール/アップグレードとしての証明書操作」がありません。
   4. CUCM で、CTI サービス/コール マネージャ サービス/CAPF サービス/TFTP サービスがダウンしています。
   5. CUCM/CAPF 証明書を再生成した場合、CTL ファイルが再生成され、必要なすべてのサービスを再起動し、Cisco Prime Collaboration Assurance で CUCM が再検出される前に新しい CAPF プロファイルが作成されていることを確認します。

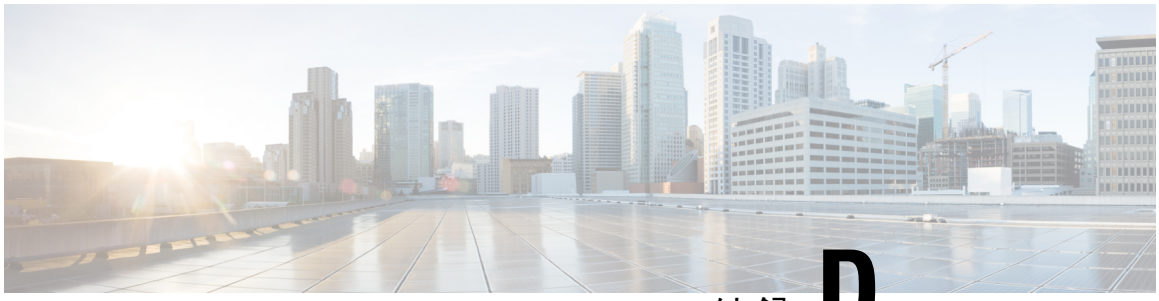
2. セッション監視の [Secure JTAPI] で Cisco Prime Collaboration Assurance を使用しているときに、エラーが発生する可能性があります。

   問題：

会議の診断でセッションが表示されない

考えられる原因：

1. JTAPI のアクセス レベルが RO（読み取り専用）ではない可能性があります。
2. エンドポイントが完全な可視性ではない可能性があります。
3. エンドポイントが JTAPI ユーザによって制御されていない可能性があります。



付録 D

Jetty および Tomcat サーバの TLS 設定

このセクションでは、次を実行するための手順を説明します。

- Cisco Prime Collaboration Assurance のクライアント接続で最小 TLS バージョンの有効化 （761 ページ）
- Jetty サーバで TLS プロトコルの有効化 （762 ページ）
- Tomcat サーバで TLS プロトコルの有効化 （762 ページ）

Cisco Prime Collaboration Assurance のクライアント接続で最小 TLS バージョンの有効化

Cisco Prime Collaboration Assurance クライアント インターフェイスの最小 TLS 設定の手順を次に示します。

始める前に

（注） Cisco Prime Collaboration Assurance から VOS ベースのデバイスへのすべての HTTPS 接続は、以下の設定によって制御されます。

ステップ 1 *root* ユーザとしてログインし、次のファイルを編集します。

`/opt/emms/conf/connector.xml`

ステップ 2 特定の接続タイプ（HTTPS）の <minTLSProtocol>TLSv1</minTLSProtocol> を編集します。

TLSv1 設定、TLSv1、TLSv 1.1、TLSv 1.2 が有効

TLSv1.1 設定、TLSv1.1, TLSv1.2 が有効

TLSv1.2 設定、TLSv1.2 が有効

ステップ 3 Cisco Prime Collaboration Assurance のすべてのサービスを再起動します。

Jetty サーバで TLS プロトコルの有効化

（注）
1. Jetty サーバは、デフォルトで 3 つのプロトコルをすべて有効にするように設定されています。
2. たとえば、TLS v1 プロトコルを無効にし、TLS v1.1 と TLS v1.2 のみを有効にするには、次の手順に従ってください。

ステップ 1 次のファイルを編集します。

```
/opt/jetty/etc/jetty-ssl.xml
```

ステップ 2 次のエントリを **sslContextFactory** タグに追加します。次に例を示します。

```
<Set name="IncludeProtocols"> <Array type="String"> <Item>TLSv1.1</Item> <Item>TLSv1.2</Item> </Array>
 </Set> <Set name="ExcludeProtocols"> <Array type="String"> <Item>TLSv1</Item> </Array> </Set>
```

ステップ 3 次のコマンドを使用して、Jetty サーバを再起動します。

```
systemctl restart mariadb
```

Tomcat サーバで TLS プロトコルの有効化

（注）
1. Tomcat サーバは、デフォルトで 3 つのプロトコルをすべて有効にするように設定されています。
2. たとえば、TLS v1 プロトコルを無効にし、TLS v1.1 と TLS v1.2 のみを有効にするには、次の手順に従ってください。

ステップ 1 次のファイルを編集します。

```
/opt/emms/apache-tomcat-8.5.11/conf/server.xml
```

ステップ 2 **port 8443** コネクタ タグの **sslProtocols** パラメータを **protocols** パラメータ に変更し、必要なプロトコルを有効化するよう定義します。

<Connector port="8443" protocol="HTTP/1.1" SSLEnabled="true"

maxThreads="150" scheme="https" secure="true"

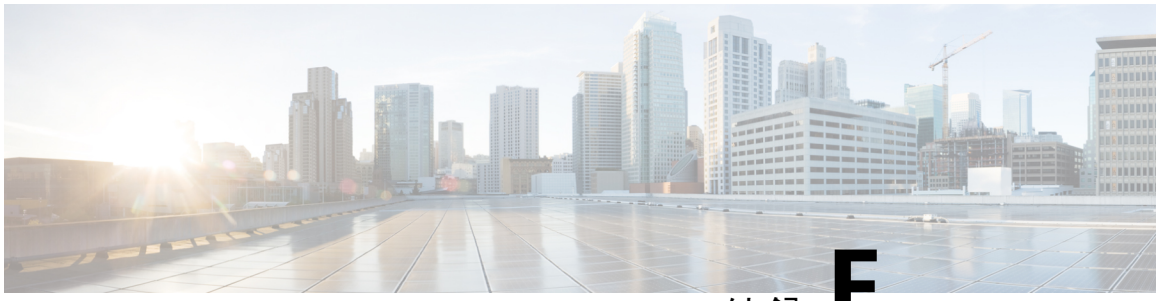
clientAuth="false" **sslProtocols="TLSv1,TLSv1.1,TLSv1.2"**

<Connector port="8443" protocol="HTTP/1.1" SSLEnabled="true"

maxThreads="150" scheme="https" secure="true"

clientAuth="false" **protocols="TLSv1.1,TLSv1.2"**

ステップ 3 上記の設定が完了した時点で、Cisco Prime Collaboration Assurance のすべてのプロセスを再起動します。



付録 E

ユーザ インターフェイス

このセクションでは、次の点について説明します。

- 概要 （765 ページ）
- フィルタ（Filters） （767 ページ）
- 拡張フィルタの開始とフィルタ基準の保存 （768 ページ）
- クイック ビュー （768 ページ）
- 製品情報の詳細の表示 （768 ページ）

概要

Cisco Prime Collaboration Assurance には、シンプルなユーザ エクスペリエンスを提供する新しいユーザ インターフェイスが用意されています。左のペインには、縦方向の展開可能な [ナビゲーション（Navigation）] タブ、[インデックス（Index）] タブ、[お気に入り （Favorites）] タブ、および [検索メニュー（Search Menu）] フィールドが表示されます。[お気に入り（Favorites）] タブでは、後で参照できるように、優先されるページにブックマークを設定できます。[Cisco Prime Collaboration Assurance] ページの [ナビゲーションの切り替え（Toggle Navigation）] アイコン をクリックすると、ダッシュレットとレポートのリストが表示されます。左上のピン アイコンをクリックすると、左側のペインの表示/非表示を切り替えることができます。

Cisco Prime Collaboration Assurance のユーザ インターフェイスでのナビゲーションの変更については、『Cisco Prime Collaboration Assurance and Analytics インストールおよびアップグレード ガイド』の「*Cisco Prime Collaboration Assurance - Advanced* ユーザ インターフェイスのナビゲーションの変更」セクションを参照してください。

[はじめに（Getting Started）] ページは、エンタープライズ モードの Cisco Prime Collaboration Assurance ユーザ インターフェイスのホーム ページです。MSP モードの [はじめに（Getting Started）] ページの詳細については、Cisco Prime Collaboration Assurance を開始する （51 ページ）を参照してください。

Cisco Prime Collaboration リリース 11.6 以降の場合

（注） 15 分にわたってアクティビティがないと、セッション タイムアウトになります。

次に、Cisco Prime Collaboration Assurance サーバでタイム アウトにならないページのリストを示します。

- システム ビュー（**System View**）
- カスタマー サマリ ダッシュボード（**Customer Summary Dashboard**）（**MSP** モードの場合）
- 診断テスト（**Diagnostics Test**）ページ、（（**UC**アプリケーション合成テスト（**UC Application Synthetic Test**）、音声電話機の機能テスト（**Audio Phone Features Test,**）、ビデオテスト（**Video Test**）、バッチテスト（**Batch Test**））
- エンドポイントの診断（**Endpoint Diagnostics**）
- パフォーマンス ダッシュボード（**Performance dashboards**）
- セッションの診断（**Session Diagnostics**）
- **All Topology** ページ （pages）

Cisco Prime Collaboration リリース **11.5** 以降の場合

（注） 15 分にわたってアクティビティがないと、会議はタイム アウトになります。

次に、Cisco Prime Collaboration Assurance サーバでタイム アウトにならないページのリストを示します。

- ネットワーク正常性の概要（**Network Health Overview**）
- カスタマー サマリ ダッシュボード（**Customer Summary Dashboard**）（**MSP** モードの場合）
- 診断テスト（（**Diagnostics Test**）、ページ（**UC**アプリケーション合成テスト（**UC Application Synthetic Test**）、音声電話機の機能テスト（**Audio Phone Features Test,**）、ビデオテスト（**Video Test**）、バッチテスト（**Batch Test**））
- エンドポイントの診断（**Endpoint Diagnostics**）
- パフォーマンス ダッシュボード（**Performance dashboards**）
- 会議の診断（**Conference Diagnostics**）
- **All Topology** ページ （pages）

フィルタ（Filters）

フィルタ機能を使用して、Cisco Prime Collaboration Assurance のユーザ インターフェイスに関する特定の情報を表示できます。データが表形式で表示されるときは常に [Filter] アイコン が表示されます。

次に、Cisco Prime Collaboration Assurance クライアントで使用可能なフィルタのタイプを示します。

- クイックフィルタ
- 高度なフィルタ

クイック フィルタおよび拡張フィルタは、大文字と小文字を区別しません。これらのフィルタについては、次のワイルドカード表現も使用できます。

- 疑問符（?）：任意の 1 文字に一致します。
- アスタリスク（*）：0 個以上の文字と一致します。

クイック フィルタ

このフィルタを使用すると、フィルタを特定のテーブル列に適用することで、テーブル内のデータを絞り込むことができます。このフィルタとともに使用される演算子は、*Contains* です。さまざまな演算子を適用するには、[Advanced Filter] オプションを使用します。

クイック フィルタを起動するには、[Filter] ドロップダウン メニューから [Quick Filter] を選択します。

クイック フィルタをクリアするには、[Filter] をクリックします。

拡張フィルタ

このフィルタを使用すると、Does not contain、Does not equal、Ends with、Is empty など、複数の演算子を使用してフィルタを適用することによって、表内のデータを絞り込むことができます。

ドロップダウン メニューからフィルタ パターン（テーブル列名）と演算子を選択します。さらに、Cisco Prime Collaboration Assurance データベースで利用可能なデータに基づいてフィルタ条件を入力する必要があります。

拡張フィルタを起動するには、[フィルタ（Filter）] ドロップダウン メニューから [拡張フィルタ（Advanced Filter）] を選択します。

拡張フィルタをクリアするには、[Filter] をクリックします。

拡張フィルタの開始とフィルタ基準の保存

拡張フィルタを起動するには、[Filter] ドロップダウン メニューから [Advanced Filter] を選択します。

拡張フィルタで使用するフィルタ基準を保存できます。

フィルタ基準を保存するには、次のようにします。

ステップ 1 [Filter] ドロップダウン メニューから、[Advanced Filter] を選択します。

ステップ 2 拡張フィルタ基準を入力します。

ステップ 3 [Go] をクリックし、次に [Save] アイコンをクリックします。

ステップ 4 [Save Preset Filter] ページで、プリセット フィルタの名前を入力して、[Save] をクリックします。

拡張フィルタをクリアするには、**[Filter]** ボタンをクリックします。

Cisco Prime Collaboration Assurance には、データをフィルタリングするための定義済みのキーワードが用意されています。さらに、保存した拡張フィルタ基準も、[Preset Filter] ドロップダウン リストにリストされます。フィルタ基準を保存する方法の詳細については、「フィルタ（Filters）」の「拡張フィルタ」を参照してください。

この機能は、[Device Management]、[Alarm ブラウザ]、および [Event ブラウザ] などの一部のページで使用可能です。プリセット フィルタを起動するには、[Show] ドロップダウン リストから使用可能な値を選択します。

Cisco Prime Collaboration Assurance には、テーブル内のデータをフィルタリングできるように、一連の定義済みフィルタが用意されています。

クイック ビュー

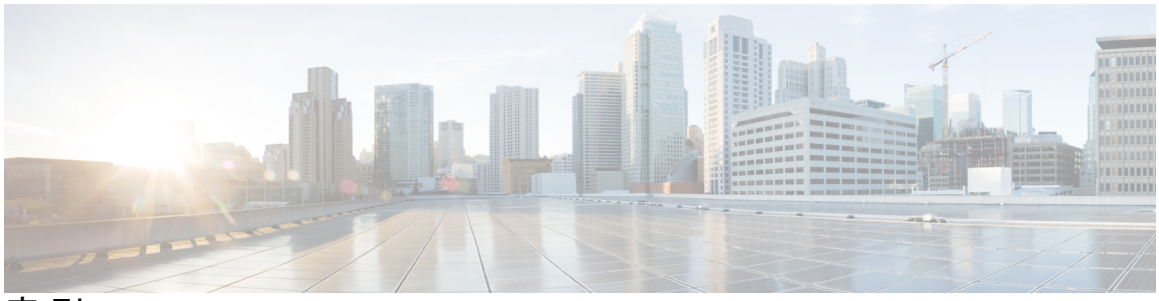
[クイック ビュー（Quick view）] アイコンは、テーブル、特定のテーブル列、またはトポロジー ペインの上にマウス ポインターを置くと表示されます。詳細を表示するページを相互起動するには、クイック ビューを使用します。Cisco Prime Collaboration Assurance では、このオプションは管理タスク、レポート、または診断ビューで使用できません。

製品情報の詳細の表示

このページには、Cisco Prime Collaboration Assurance の [About（概要）] に関する詳細が表示されます。

このページを Essential モードで表示するには、ユーザ インターフェイスの右上隅にある **[globaladmin - Essential]** > **[概要（About）]** の順にクリックします。

- [システム情報（システム情報）] リンクをクリックすると、次のシステム情報の詳細がクイック ビューで表示されます。
  - Build Version
  - License Type
  - 有効期限（有効期限前の直近 15 日間が赤色で表示）
  - IP アドレス
  - MACアドレス
  - VM キャパシティ
- [ライセンス（Licensing）] リンクをクリックし、[ライセンス管理（License Management）] ページを開きます。



索 引

記号

[LDAP サーバの設定（configure LDAP server）] 82
[デバイス検出の推奨事項（Recommendations for Device Discovery）] 142
[会議（conferences）] 573
　上位 N の会議の拠点 573

A

Assurance のユーザ ロールおよびタスク 80

C

Cisco 1040 センサー 747
Cisco 1040 のリセット 755
globaladmin 79

D

DNS 設定 751
　および Cisco 1040 751
DSP 使用率 565

E

Endpoint Utilization レポート 523

N

NANP 481
スケジュールされた会議に参加しなかったエンドポイントに関する情報が表示されます。 524

S

SMTP サーバ メッセージ 468
smuser パスワード 491, 493
Syslog 通知 249

T

TFTP サーバ 748
TFTP ダウンロード模擬テスト 597
　追加 597

U

UC システム パフォーマンス 575
UCCE 576

あ

IP SLA ping 587
アシュアランス ライセンス 67
アプリケーション、模擬テスト用に設定 594
アラーム 47
　ステータス 47

い

イベント 49, 289, 293, 294
　コール イベント 293, 294
　重大度 49
　ブラウザ 289
インターフェイスのコンポーネント 768
　クイック ビュー 768
インベントリ収集 165
　クラスタ デバイス検出 165

え

エンドツーエンド コールの模擬テスト 598
　追加 598

お

ビデオ エンドポイントのモニタリング 14

か

会議 572
ビデオ会議の統計情報 572
カスタム 464
ダッシュボード 464
管理 173
グループ 173

き

キャパシティ分析< 574
最下位 N の会議デバイス 574
キャパシティ分析 558, 559, 560, 563
上位 N CAC の帯域幅拠点 559
上位 N 煩雑時のトランク 560, 563
使用されるトランク 560
ルート グループの使用率 563
緊急コールの模擬テスト 595
追加 595

く

クラスタ デバイス検出 165
クラスタ デバイス検出、デバイス プールのしきい値用に実行 273
グループ 177
作成 177
デバイスの削除 177
デバイスの追加 177
グループ管理 558

け

ゲートウェイコードの設定 488
検出 165
クラスタ デバイス 165

こ

顧客音声ポータル 576
コンタクト センター 398, 403, 413, 422, 431
ダッシュボード 398, 403, 413, 422, 431
CUIC 422
CVP 403
MediaSense 431
UCCE 413

さ

サービス エクスペリエンス 565, 566, 567, 568, 569, 570, 571
サービス エクスペリエンスの分配 566, 567
サービス品質問題があるエンドポイント 568
サービス品質問題があるユーザ 570, 571
上位 N のコール失敗発生拠点 569, 570
問題がある 568
サービス エクスペリエンス エンドポイントに関する情報を提供します。 568

し

シード ファイル形式。<Default Para Font> インポート ファイル形式を参照 590
障害管理 15, 43, 44, 45
アラーム 44
アラーム作成 45
イベント 43
イベントの作成 44
使用頻度が最も低いエンドポイント タイプ 551
ジョブ 707, 710
キャンセル 710
スケジュール 707
Jobs 705
診断 15

す

スーパー管理者 80
スケジュール済みレポート 580

せ

セッション 317, 326, 331, 334, 335, 338, 660
360 度セッション ビュー 334
可視性 331
ダッシュボード 326
統計情報 338
トポロジ 335
トラブルシュート 660
ワークフロー 317
セッション詳細レポート 522
設定 749
Cisco 1040 749
プライマリ Service Monitor 749

た

ダイヤル プラン 481
NANP 481
デフォルト 481

つ

追加 259, 596, 753
Cisco 1040 753
アラーム セット 259
模擬テスト 596
メッセージ待機インジケータ テスト 596
追加とコピー 100
通知 248
SNMP トラップ、送信 248

て

停止 751
QOVR プロセス 751
データの入力 545
テクノロジー導入 546
テクノロジーの導入 547, 548, 549, 550
エンドポイント タイプのコール分配 549, 550
エンドポイント モデル コール分配 548, 549
エンドポイントの導入分配 547, 548
デバイス 223
検出 223
デバイス インベントリ管理 13
デバイスの追加 157
テレプレゼンス ルームの使用率 552
電子メール 249
通知 249
電話機テストの概要 644
電話ステータス テスト 592
変更 592
電話ステータス テストの作成 588
電話ステータス テストをインポート中 589

と

トラップ、SNMP 750
Cisco 1040 から、 750
トラフィック分析 554, 555, 556, 557
かけた番号の上位 N 位 555
コール トラフィック分析 557
上位 N コール トラフィック拠点 556
上位 N の発信者 554
とらふぃっくぶんせき 555
上位 N のオフネット トラフィック拠点 555
トラブルシュート 664, 676
起動 664
レポート 676

の

ノードツーノード テストの作成中 615

は

バックアップ 724
りれき 724
バックアップと復元 717
バッチテスト 640
電話テスト、タイプ 640

ひ

ビデオ コラボレーション ダッシュボード 466
カスタマイズ 466
ビデオ パス分析 681
ビデオ会議 571, 572

ふ

ファイル、センサー固有の設定 754
不参加の会議 552, 553
分析 39, 56, 68, 539, 540
使用シナリオ 56
ユーザーインターフェイス 539, 540
詳細分析 540
ユーザ インターフェイス 539, 540
クイック ビュー 539
グローバル フィルタ オプション 540
ライセンス 68

ほ

ポーリングとしきい値 240
パラメータ、管理 240
表示 240

め

メッセージ待機インジケータの模擬テスト 597
Cisco Unified CallManager のアップグレード後の障害 597

も

模擬テスト、使用 **592, 593, 594, 601**
緊急コール テスト **593**
エンドツーエンド コール テスト **593**
Cisco Unity メッセージ待機インジケータ テスト、概要 **594**
Dial-Tone テスト **592**
TFTP ダウンロード テスト **593**
テストの追加 **601**
ダイヤル トーン **601**
Phone Registration テスト **592**

ゆ

有効化 **750**
コール メトリックのアーカイブ **750**
ユーザ アカウント **79**
ユーザの削除 **81, 82**
ユーザの詳細の編集 **81, 82**

ら

らいせんすしよう **576**

れ

レポート **16**

ろ

ロールおよびタスク、マッピング **80**

ん

インターフェイス コンポーネント **767**
フィルタ **767**