



Cisco Packaged Contact Center Enterprise インストレーション/ アップグレードガイド、リリース 10.5(1)

初版：2014年06月18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。

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザ側の責任になります。

対象製品のソフトウェア ライセンスおよび限定保証は、製品に添付された『Information Packet』に記載されています。添付されていない場合には、代理店にご連絡ください。

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.

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよびこれら各社は、商品性の保証、特定目的への準拠の保証、および権利を侵害しないことに関する保証、あるいは取引過程、使用、取引慣行によって発生する保証をはじめとする、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、シスコおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド出力、ネットワーク トポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際の IP アドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

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: <http://www.cisco.com/go/trademarks>. 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. (1110R)

© 2014 Cisco Systems, Inc. All rights reserved.



目次

はじめに **xiii**

変更履歴 **xiii**

このマニュアルについて **xiv**

対象読者 **xiv**

マニュアルの構成 **xv**

関連資料 **xv**

フィールドアラートおよびフィールド通知 **xvi**

マニュアルに関するフィードバック **xvi**

表記法 **xvi**

準備 **1**

システム要件 **3**

ソリューションのコンポーネント **4**

ハードウェア要件 **5**

VMware ホスティング **6**

基本設定およびユーティリティ ツール **6**

Cisco Systems Contact Center コンポーネント **7**

サードパーティ製ソフトウェア **7**

ソフトウェア ライセンス **9**

サポートされるブラウザ **10**

カスタマー サイト サーバの準備 **11**

Cisco USC C シリーズ カスタマー サイト サーバの準備 **11**

C240 MS3 TRC#1 の RAID の設定 **11**

VMware vSphere ESXi のインストール **13**

vCenter へのカスタマー ESXi ホストの追加 **13**

RAID Config Validator ユーティリティの実行 **14**

Cisco UCS B シリーズ カスタマー サイト サーバの準備 **15**

ファブリック インターコネクットの要件	15
Cisco UCS B シリーズ ブレードの要件	17
vNIC の要件	17
vHBA の要件	18
SAN プロビジョニング用の Packaged CCE アプリケーション IOPS	19
NTP および時刻同期	21
Cisco UCS B シリーズ サーバのタイムゾーンと NTP タイムサーバの設定	23
ネットワーク設計の考慮事項	25
Cisco UCS C シリーズ サーバのネットワーク要件	25
Cisco UCS C シリーズ サーバ用の VMware vSwitch の設計	27
UCSC シリーズ サーバイーサネットアップリンク用のデータセンタースイッチの設定	27
Cisco UCS B シリーズ サーバのネットワーク要件	29
Cisco UCS B シリーズ サーバ用の VMware vSwitch の設計	30
Cisco UCS B シリーズ ファブリック インターコネク トイーサネットアップリンク用のデータセンター スwitch の設定	33
帯域幅のプロビジョニングおよびネットワーク QoS の考慮事項	40
インストール : ゴールデン テンプレートと直接インストール	41
インストール シナリオ	41
インストールのシナリオ	41
ゴールデン テンプレートの作成	43
ゴールデン テンプレートについて	43
ゴールデン テンプレートの作成	44
Cisco Unified Contact Center Enterprise コールサーバ用のゴールデンテンプレートの作成	44
Cisco Unified Contact Center Enterprise データサーバ用のゴールデンテンプレートの作成	44
Cisco Unified Customer Voice Portal サーバ用のゴールデンテンプレートの作成	45
Unified CVP Reporting Server 用のゴールデンテンプレートの作成	46
Cisco Unified Communications Manager 用のゴールデンテンプレートの作成	47
Cisco Finesse 用のゴールデンテンプレートの作成	47

Cisco Unified Intelligence Center 用のゴールデン テンプレートの作成	47
カスタマー サイトでのゴールデン テンプレートの展開	49
ホストの権限	49
自動ツール	49
エクスポート用の自動化スプレッドシートへの入力	50
エクスポート用の自動化スクリプトの実行	51
カスタマーへの転送	52
カスタマー サイトの準備状態の確認	52
インポート用のスプレッドシートへの入力	53
インポート用の自動化スクリプトの実行	58
ゴールデン テンプレートのインポート後	61
データ サーバのインポート後の手順	61
コール サーバのインポート後の手順	62
Cisco Unified Voice Portal のインポート後の手順	62
Cisco Unified Communications Manager のインポート後の手順	62
Cisco Unified Intelligence Center のインポート後の手順	63
Cisco Finesse のインポート後の手順	63
インポート後の手順	63
ネットワーク アダプタ設定と電源投入の検証	63
Cisco Diagnostic Framework Portico の設定	64
Unified CCE 暗号化ユーティリティの設定	64
ドメイン ユーザの追加	65
レジストリ設定の編集と VM の再起動	66
ネットワーク アダプタの名前の変更と再バインド	66
セキュリティ ウィザードの実行	68
時刻源のリセット	68
Unified Communications Manager パブリッシャの設定	69
サブスクリバを追加するための Unified Communications Manager パブリッシャ の起動	69
Unified Communications Manager サブスクリバの設定	70
Unified Intelligence Center パブリッシャの設定	70
オンラインでのライセンスの取得	71

サブスクリバを追加するためのパブリッシャの起動	72
サブスクリバの設定	72
Cisco Finesse プライマリ ノードの設定	73
セカンダリ ノードの設定	73
セカンダリ Finesse を設定するための Finesse 管理コンソールの起動	74
カスタマイズ中のパスワード変更	74
直接インストール	75
直接インストールについて	75
Cisco Unified Contact Center Enterprise コール サーバ用の VM の作成	76
Cisco Unified Contact Center Enterprise データ サーバ用の VM の作成	76
Cisco Unified Customer Voice Portal サーバ用の VM の作成	77
Cisco Unified Communications Manager パブリッシャ用の VM の作成	78
Cisco Unified Communications Manager サブスクリバ用の VM の作成	78
Cisco Finesse プライマリ用の VM の作成	79
Cisco Finesse セカンダリ用の VM の作成	79
Cisco Unified Intelligence Center パブリッシャ用の VM の作成	80
Cisco Unified Intelligence Center サブスクリバの VM の作成	80
Cisco Unified CVP Reporting Server 用の VM の作成	80
ゴールデン テンプレートと直接インストール用の共通タスク	83
Open Virtualization ファイル	83
ISO ファイルのマウントおよびアンマウント	83
OVA からの仮想マシンの作成	85
DNS サーバの設定	87
データベース ドライブの設定	87
アンチウイルス ソフトウェアのインストール	88
ゴールデン テンプレートと直接インストール用のソフトウェア インストール	89
Windows Server 2008 のインストール	89
Windows での VM の VMware ツールのインストール	91
コール サーバおよびデータ サーバのネットワーク アダプタの設定	91
Windows アップデートの実行	93
Microsoft SQL Server のインストール	93
ローカリゼーションの照合順序とロケールの設定	96

Cisco Unified Contact Center Enterprise のインストール	98
Cisco Unified CVP サーバのインストール	98
Cisco Unified CVP のネットワーク アダプタの設定	99
Cisco Unified CVP Reporting Server のインストール	99
データベース ドライブの設定	101
外部 AW-HDS-DDS のインストールおよび設定	101
外部 AW-HDS-DDS の設定	102
外部 AW-HDS-DDS の HDS データベースの作成	104
VOS ベースのコンタクトセンターアプリケーションに対するゴールデンテンプレートのインストール	104
VOS ベースのコンタクトセンターアプリケーションのパブリッシャ/プライマリ ノードに対する直接インストール	105
Cisco Unified Communications Manager 用のクラスタの設定	107
Cisco Unified Communications Manager のサービス構成設定	108
Cisco Unified Communications Manager パブリッシャのインストール	108
VOS ベースのコンタクトセンター アプリケーションのサブスクリバ/セカンダリ ノードに対する直接インストール	109
Cisco Unified Intelligence Center 用のクラスタの設定	111
Cisco Finesse のクラスタの設定	111
設定	113
Cisco Unified CCE データ サーバ	115
SQL Server の設定	115
ドメイン マネージャの設定	116
インスタンスのセットアップ	117
ロガーの設定	117
ロガー データベースおよびログの設定	117
Web セットアップのロガー コンポーネントの設定	118
基本設定の適用	119
ICMDBA ツールを使用した基本設定の実行	120
AW データベースおよびログの設定	122
管理サーバおよびリアルタイム データ サーバのコンポーネントの設定	123
Unified Intelligence Center の SQL ユーザ アカウントの設定	124

Cisco Unified CCE コール サーバ	127
Unified CCE ルータの設定	128
Generic PG の追加	128
PIM1 の追加 (CUCM PIM)	129
PIM2 の追加 (最初の VRU PIM)	130
PIM3 の追加 (2 番目の VRU PIM)	131
PIM4 の追加 (3 番目の VRU PIM)	132
PIM5 の追加 (4 番目の VRU PIM)	133
PIM の作成後	133
CTI サーバの設定	135
JTAPI のインストール	136
メディア ルーティング ペリフェラル ゲートウェイの設定	136
メディア ルーティング PG の追加	137
CTI OS サーバの設定	138
Cisco Unified Customer Voice Portal	141
ネットワーク カードの検証	142
Unified CVP コール サーバの設定	142
Unified CVP VXML サーバの設定	143
ゲートウェイの設定	144
Unified CVP Media Server の設定	144
スクリプトおよびメディア ファイルの転送	145
ライセンス ファイルの転送	145
SNMP の設定	146
SIP サーバ グループの設定	146
ダイヤル番号パターンの設定	147
Location-Based コール アドミッション制御	149
Cisco IOS Enterprise 音声ゲートウェイの設定	151
Cisco IOS Enterprise 音声ゲートウェイの設定	151
Cisco Unified Communications Manager	157
Unified Communications Manager ライセンス	158
ライセンスの生成と登録	158
ライセンスのインストール	159

サービスのアクティブ化	159
完全修飾ドメイン名の設定	160
Cisco Unified Communications Manager グループの設定	160
会議ブリッジの設定	161
メディアターミネーションポイントの設定	162
トランスコーダの設定	162
メディアリソースグループの設定	163
メディアリソースグループリストの設定および関連付け	164
CTI ルートポイントの設定	164
アプリケーションユーザの設定	165
SIP オプションの設定	165
トランクの設定	165
ルートグループの設定	166
ルートリストの設定	167
ルートパターンの設定	167
展開タイプの設定	169
展開タイプの設定	169
Cisco Unified Intelligence Center	171
Unified Intelligence Center データソースの設定	171
レポートバンドルのダウンロード	173
レポートバンドルのインポート	174
Unified Intelligence Center Administration の設定	174
Cisco Finesse	177
Cisco Finesse プライマリ ノードでの CTI サーバの設定	177
Unified Contact Center Enterprise 管理およびデータサーバの設定	178
Tomcat の再起動	178
デフォルトのデスクトップレイアウトのエージェントキュー統計情報ガジェットの有効化	178
ライブデータレポート	179
ライブデータの前提条件	179
Finesse へのライブレポートの追加	180
デフォルトデスクトップレイアウトへのライブレポートの追加	180

カスタム デスクトップ レイアウトへのライブ レポートの追加	181
チーム レイアウトへのライブ レポートの追加	183
Finesse のライブ データ ストック レポートの変更	185
Cisco Unified Customer Voice Portal Reporting Server	187
CVP OAMP での CVP Reporting Server の設定	188
Unified CVP レポーティング ユーザ	188
LDAP ユーザ用の Active Directory サーバのセットアップ	188
Cisco Unified Customer Voice Portal レポート テンプレートの取得	188
Cisco Unified CVP レポート データのデータ ソースの作成	189
Unified Intelligence Center への CVP レポート テンプレートのインポート	191
バージョンのアップグレード	193
リリース 10.5(1) へのアップグレード	195
アップグレードの準備	195
アップグレードの順序	196
Cisco Finesse のアップグレード	197
アップグレードの実行	197
DVD/CD からの Finesse のアップグレード	198
リモート ファイルシステムからの Finesse のアップグレード	198
デスクトップ レイアウトのアップグレード後の作業	199
Cisco Unified Customer Voice Portal および Unified CVP Reporting のアップグレード	200
アップグレード前の作業	200
アップグレード	200
Cisco Unified CVP Operations Console のアップグレード	200
Cisco Unified CVP コール サーバのアップグレード	201
アップグレード ファイルの取得と適用	202
Reporting Server のアップグレード	202
ゲートウェイ Cisco IOS バージョンのアップグレード	203
Cisco Unified Contact Center データ サーバおよびコール サーバのアップグレード	204
アップグレード前の作業	204
設定変更を無効にする	204

パスワードの特定	204
拡張データベース移行ツールのダウンロード	204
A 側のアップグレード	205
A 側のデータ サーバ、コール サーバ、外部 AW のサービスの停止	205
データ サーバ データベースのアップグレード	205
データ サーバのセットアップの実行	206
Cisco Unified CCE コール サーバのセットアップの実行	207
Cisco CTI OS サーバのセットアップの実行	207
B 側のサービスと任意の外部 AW-HDS-DDS のシャットダウン	208
A 側の起動および動作の確認	208
B 側のアップグレード	208
データ サーバ データベースのアップグレード	208
データ サーバのセットアップの実行	209
Cisco Unified CCE コール サーバのセットアップの実行	209
Cisco CTI OS サーバのセットアップの実行	210
B 側を起動します。	210
外部 AW-HDS-DDS のアップグレード	210
外部 AW-HDS-DDS データベースのアップグレード	210
外部 AW-HDS-DDS のセットアップの実行	211
アップグレード後の作業	211
設定変更の再有効化	211
自動へのサービスの設定	212
新しい言語パックのインストール	212
Cisco Unified Intelligence Center のアップグレード前	212
COP ファイルのダウンロードとインストール	212
Cisco Unified Intelligence Center を更新するためのユーティリティの実行	213
システムの検証およびシステム インベントリの構築	213
Cisco Unified Intelligence Center のアップグレード	214
アップグレード	214
アップグレードについて	214
アップグレード ファイルのダウンロード	215
DVD/CD からの Cisco Unified Intelligence Center のアップグレード	215

リモート ファイル システムからの Cisco Unified Intelligence Center のアップグレード	216
Cisco Unified Communications Manager のアップグレード	216
アップグレード前の作業	216
アップグレード	217
DVD/CD からの Cisco Unified Communications Manager のアップグレード	217
リモート ファイル システムからの Cisco Unified Communications Manager のアップグレード	217
ソフトウェア バージョンの切り替え	218
コール サーバでの JTAPI のアップグレード	218
ライセンス	219
アップグレードライセンス	219
VMware 設定ユーティリティのアップグレード	220
オプション : VMware vSphere ESXi のアップグレード	221
参考資料	223
基本設定の更新	223
言語パックのインストール	229
簡易ネットワーク管理プロトコル	229
Cisco Unified Communications Manager のサービス構成設定	230
ライブ データの証明書	231
ライブ データの自己署名証明書の追加	231
ライブ データの CA 証明書の取得およびアップロード	232
内部的な証明書の作成	233
Microsoft Certificate Server のセットアップ	233
CA 証明書のダウンロード	234
Internet Explorer のルート証明書の導入	235
Internet Explorer ブラウザの証明書のセットアップ	235
Firefox ブラウザの証明書のセットアップ	236



はじめに

- [変更履歴, xiii ページ](#)
- [このマニュアルについて, xiv ページ](#)
- [対象読者, xiv ページ](#)
- [マニュアルの構成, xv ページ](#)
- [関連資料, xv ページ](#)
- [フィールドアラートおよびフィールド通知, xvi ページ](#)
- [マニュアルに関するフィードバック, xvi ページ](#)
- [表記法, xvi ページ](#)

変更履歴

次の表に、このガイドに対する変更のリスト、リンク、これらの変更が行われた日付を示します。最新の変更から順に表示されています。

変更	日付	Link
リリース 10.5(1) 用のマニュアルの初版	06/18/2014	

変更	日付	Link
<p>MR PG は 4 つまでの PIM に対応します。</p> <ul style="list-style-type: none"> • 1 つのアウトバウンド PIM • SocialMiner に対する 1 つのマルチチャネル PIM • E-Mail Interaction Manager / Web Interaction Manager に対する 1 つのマルチチャネル PIM • サードパーティのマルチチャネルアプリケーションに対する 1 つのマルチチャネル PIM 		メディアルーティングペリフェラルゲートウェイの設定, (136 ページ)
<p>Cisco Packaged CCE の展開は、Cisco UCS B シリーズブレードサーバでサポートされます。</p>		システム要件, (3 ページ) カスタマーサイトサーバの準備, (11 ページ) ネットワーク設計の考慮事項, (25 ページ)

このマニュアルについて

このマニュアルでは、Packaged CCE のインストール、設定、およびアップグレードの方法について説明します。

Cisco Packaged Contact Center Enterprise (Packaged CCE) は、仮想化環境で Cisco Unified Contact Center Enterprise を提供するためのソリューション展開です。Packaged CCE では、容量制限に厳守する必要があります。http://www.cisco.com/en/US/products/ps12586/prod_technical_reference_list.html で入手できる『Cisco Packaged Contact Center Enterprise Design Guide』で詳しく説明されています。設計ガイドに記載されているすべてのルールおよび要件に従うことが必要です。

このマニュアルでは、Packaged CCE の試験限定の導入について説明していません。その導入については、Packaged CCE の wiki (http://docwiki.cisco.com/wiki/Packaged_CCE) を参照してください。

対象読者

このマニュアルは、シスココンタクトセンターアプリケーションに関する専門知識があり、VMware テクノロジーを使用した仮想マシンの導入および管理に関する経験が豊富な、Packaged CCE を実装するパートナーおよびサービスプロバイダーを対象としています。

マニュアルの構成

セクション	内容
パート I: 準備, (1 ページ)	システム要件 ソリューションのコンポーネント カスタマー サイトの準備 ネットワーク設計の考慮事項
パート II: インストール: ゴールデンテンプレートと直接インストール, (41 ページ)	2つのインストール オプションの手順: <ul style="list-style-type: none"> • ゴールデン テンプレートを作成し、エクスポート用に処理するための方法 • 仮想マシンを直接作成する方法
パート III: 設定, (113 ページ)	カスタマー サイトでシスコ コンタクト センター 製品を設定するための方法
パート IV: バージョンのアップグレード, (193 ページ)	アップグレード要件および手順
付録: 参考資料, (223 ページ)	基本設定の更新 言語パックのインストール 簡易ネットワーク管理プロトコル Unified CM のサービス構成設定 Live Data の証明書

関連資料

製品名	リンク
Cisco Packaged Contact Center Enterprise	http://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/tsd-products-support-series-home.html
Cisco Unified Contact Center Enterprise	http://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/tsd-products-support-series-home.html

製品名	リンク
Cisco Unified Communications Manager	http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/tsd-products-support-series-home.html
Cisco Unified Intelligence Center	http://www.cisco.com/c/en/us/support/customer-collaboration/unified-intelligence-center/tsd-products-support-series-home.html
Cisco Finesse	http://www.cisco.com/c/en/us/support/customer-collaboration/finesse/tsd-products-support-series-home.html
Customer Voice Portal (CVP、旧 ISN)	http://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/tsd-products-support-series-home.html

フィールドアラートおよびフィールド通知

シスコ製品が変更されたり、主要なプロセスが重要であると判断される場合があります。これらは、Cisco Field Alert および Cisco Field Notice メカニズムを使用して通知されます。Cisco.com の Product Alert Tool からフィールドアラートとフィールド通知を受信するように登録できます。このツールにより、関心のある製品をすべて選択することで通知を受信するようにプロフィールを作成できます。Cisco.com にログインして、次の URL からツールにアクセスします。

<http://www.cisco.com/cisco/support/notifications.html>

マニュアルに関するフィードバック

このマニュアルに関する技術的なフィードバック、または誤りや記載もれなどお気づきの点がございましたら、HTML ドキュメント内のフィードバック フォームよりご連絡ください。ご協力をよろしくお願いいたします。

mailto:contactcenterproducts_docfeedback@cisco.com

表記法

このマニュアルでは、次の表記法を使用しています。

表記法	説明
太字	<p>アイコン、ボタン名、ダイアログボックス名など、画面に表示される項目は、[] で囲んで表示しています。次に例を示します。</p> <ul style="list-style-type: none"> • [編集 (Edit)] > [検索 (Find)] を選択します。 • [終了 (Finish)] をクリックします。
イタリック体	<p>イタリック体は、次の場合に使用しています。</p> <ul style="list-style-type: none"> • 新しい用語の紹介。例：スキルグループとは、類似したスキルを持つエージェントの集合です。 • 強調。例：数字の命名規則は使用しないでください。 • ユーザが置き換える必要がある構文値。例：IF (<i>condition, true-value, false-value</i>) • ドキュメントのタイトル。例：『Cisco Unified Contact Center Enterprise Installation and Upgrade Guide』を参照してください。
window フォント	<p>Courier などのウィンドウ フォントは、次の場合に使用されます。</p> <ul style="list-style-type: none"> • コード中のテキストや、ウィンドウに表示されるテキスト。例： <pre><html><title>Cisco Systems, Inc. </title></html></pre>
< >	<p>山カッコは、次の場合に使用されます。</p> <ul style="list-style-type: none"> • コンテキストでイタリックが許可されない引数 (ASCII 出力など)。 • ユーザが入力する文字列で、ウィンドウには表示されないもの (パスワードなど)。



第 **II** 部

準備

- システム要件, 3 ページ
- カスタマー サイト サーバの準備, 11 ページ
- ネットワーク設計の考慮事項, 25 ページ



第 1 章

システム要件

- [ソリューションのコンポーネント, 4 ページ](#)
- [ハードウェア要件, 5 ページ](#)
- [VMware ホスティング, 6 ページ](#)
- [基本設定およびユーティリティ ツール, 6 ページ](#)
- [Cisco Systems Contact Center コンポーネント, 7 ページ](#)
- [サードパーティ製ソフトウェア, 7 ページ](#)
- [ソフトウェア ライセンス, 9 ページ](#)
- [サポートされるブラウザ, 10 ページ](#)

ソリューションのコンポーネント

Cisco Packaged CCE コンタクトセンターアプリケーションは次のとおりです。

Cisco Unified CCE コール サーバは、コールルータとして機能し、すべてのルーティング決定を行います。Peripheral GatewayおよびCTIOSオブジェクトサーバとしても動作します。

Cisco Unified CCE データ サーバは、ロガーとして機能し、コンタクトセンターの設定データおよびレポートデータデータを保存します。管理およびリアルタイムデータサーバ（またはAW）としても動作します。

Cisco Unified Customer Voice Portal (CVP) コール サーバは、プロンプト、キューイング、およびコール制御を提供します。Packaged CCE の場合、CVP サーバはコールサーバとVXMLサーバの機能を組み合わせています。このマニュアルでは、Unified CVP コール/VXMLサーバとして言及します。

Cisco Unified Communications Manager サーバは、コール処理コンポーネントです。パブリッシャは読み取り書き込みデータベースを保存します。電話やゲートウェイなどのデバイスは、サブスクリバに登録します。

Cisco Unified CVP OAMP Server。Unified CVP クラスタを維持します。

Cisco Unified CVP Reporting Server。CVP コンポーネントとコールサーバから情報を収集し、Cisco Unified Intelligence Center でその情報を使用できるようにします。

Cisco Unified Intelligence Center。Webベースのレポートアプリケーションで、Unified Contact Center Enterprise および Cisco Unified CVP のリアルタイムおよび履歴レポートを生成します。

Cisco Finesse。ブラウザベースのエージェントおよびスーパーバイザデスクトップです。

これらの VM は、下記のように A 側 B 側の両方に存在する必要があります。

A 側に必要な VM	B 側に必要な VM
Unified CCE コール サーバ	Unified CCE コール サーバ
Unified CCE データ サーバ	Unified CCE データ サーバ
Unified CVP コール/VXML サーバ 1A	Unified CVP コール/VXML サーバ 1B
Unified CVP コール/VXML サーバ 2A	Unified CVP コール/VXML サーバ 2B
Unified CVP OAMP サーバ	—
Unified Intelligence Center パブリッシャ	Unified Intelligence Center サブスクリバ
Finesse プライマリ	Finesse セカンダリ

Unified Communications Manager パブリッシャ サーバとサブスライバは、展開の一環として展開されている必要があります。A 側と B 側に存在する VM、または外部マシンとして設定できます。Unified CVP Reporting Server の VM は、オプションです。

A 側の他の VM	B 側の他の VM
Unified Communications Manager パブリッシャ	Unified Communications Manager サブスライバ 2
Unified Communications Manager サブスライバ 1	Unified CVP Reporting Server (任意)



(注) 外部の Unified Communications Manager クラスタを使用している場合でも、追加の VM を使用することはできません。

ハードウェア要件

カスタマーサイトの Packaged CCE の展開では、ペアの Unified Computing System (UCS) サーバを使用したデュプレックス環境で実行する必要があります。これらのサーバは、A 側ホストおよび B 側ホストと呼ばれます。

新規インストールまたは技術更新については、Packaged CCE は Unified Computing System (UCS) C240 M3S TRC#1 および the B200 M3 TRC#1 の両方をサポートします。

- C240 M3S : http://docwiki.cisco.com/wiki/UC_Virtualization_Supported_Hardware#C240_M3S_.28SFF.29_TRC.231
- B200 M3 TRC#1 : http://docwiki.cisco.com/wiki/UC_Virtualization_Supported_Hardware#B200_M3_TRC.231

共通アップグレードについては、Packaged CCE は Unified Computing System (UCS) C240 M3S TRC#1 および C260 M2 TRC#1 サーバの両方を継続してサポートします。

- C240 M3S : http://docwiki.cisco.com/wiki/UC_Virtualization_Supported_Hardware#C240_M3S_.28SFF.29_TRC.231
- C260 M2 : http://docwiki.cisco.com/wiki/UC_Virtualization_Supported_Hardware#C260_M2_TRC.231

Packaged CCE を UCS B200 M3 TRC#1 と注文する場合、お客様はデータセンター内にサポートされる UCS B シリーズプラットフォーム インフラストラクチャおよび SAN をすでに持っているか、これらを別々に購入する必要があります。UCSB シリーズブレードは、スタンドアロンサーバではなく、内部ストレージはありません。



重要 2つの Packaged CCE サーバは同じサーバ モデルを使用する必要があります。

VMware ホスティング

新規インストールまたは技術更新は以下のサーバのいずれかで展開できます。

- VM Version 8 上で ESXi 5.5 または ESXi 5.1 を持つ C240 M3S TRC#1
- VM Version 8 上で ESXi 5.5 または ESXi 5.1 を持つ B200 M3 TRC#1

共通アップグレードは以下のサーバのいずれかで展開できます。

- VM Version 8 上で ESXi 5.5 または ESXi 5.1 を持つ C260 M2 TRC#1
- VM Version 8 上で ESXi 5.5 または ESXi 5.1 を持つ C240 M3S TRC#1

基本設定およびユーティリティ ツール

ソフトウェア	注記	ダウンロード
CCEPACM1BaseConfig_10.5.1.zip	このソフトウェアは自動的に、各 PCCE の導入に必要な特定の要素を設定します。	http://software.cisco.com/download/type.html?mdfid=284360381&i=rm で [ソフトウェアのダウンロード (Download Software)] サイトに移動します。 設定スクリプトのリンクをクリックします。 次に、基本設定スクリプトの zip ファイルを選択します。
Domain_Update_Tool.zip	このツールは、基本設定をインストールした後でデータベースに保存されているドメイン名を変更するために必要になります。	http://software.cisco.com/download/type.html?mdfid=284360381&i=rm で [ソフトウェアのダウンロード (Download Software)] サイトに移動します。 設定スクリプトのリンクをクリックします。 次に、ドメイン名を変更するユーティリティを選択します。

Cisco Systems Contact Center コンポーネント



注目 Packaged CCE 10.5(1) は、Packaged CCE 展開でサポートされないコンポーネントを複数含む Unified CCE 10.5(1) と同じメディア キットを共有します。加えて、10.5(1) メディア キットには Packaged CCE 10.5 展開では使用されないリリース 10.0(1) であるコンポーネントが含まれます。Packaged CCE 10.5(1) を展開する場合、リリース 10.5(1) ソフトウェアのみ使用してください。

コンポーネント	メジャー リリース バージョン	オペレーティング システム
Cisco Unified Contact Center Enterprise	10.5(1) 以降のメンテナンス リリース	Microsoft Windows
Cisco Unified Customer Voice Portal	10.5(1) 以降のメンテナンス リリース	Microsoft Windows
Cisco Unified Communications Manager	10.5(1) 以降のメンテナンス リリース 10.0(1) 以降のメンテナンス リリース	Linux ベースの Cisco Unified Communications オペレーティング システム
Cisco Unified Intelligence Center	10.5(1) 以降のメンテナンス リリース	Linux ベースの Cisco Unified Communications オペレーティング システム
Cisco Finesse	10.5(1) 以降のメンテナンス リリース	Linux ベースの Cisco Unified Communications オペレーティング システム

オプション :

Cisco Unified E-Mail Interaction Manager/Web Interaction Manager - 9.0(1) 以降のメンテナンス リリース

Cisco SocialMiner - 10.5(1) 以降のメンテナンス リリース

Cisco MediaSense - 10.5(1) 以降のメンテナンス リリース

サードパーティ製ソフトウェア

このセクションでは、仮想化されたコンタクトセンターモジュールを提供するために必要なサードパーティ製ソフトウェアについて示します。



(注) サードパーティ製ソフトウェアの要件は、ゴールデン テンプレートと直接インストールの両方が対象です。

ソフトウェア	バージョン	注記
Microsoft Windows Server 2008 R2 Standard Edition	Service Pack 1	<p>用途 :</p> <ul style="list-style-type: none"> • Unified CCE コール サーバ • Unified CCE データ サーバ • Unified CVP Call/VXML Server • Unified CVP OAMP Server • Unified CVP Reporting Server <p>(注) Windows Server 2008 リモートデスクトップはソフトウェアのインストールまたはアップグレードではサポートされていません。</p>
Microsoft Windows Active Directory	Windows Server 2003、2008、2012	<p>Windows Server Active Directory サポートには R2 バージョンが含まれています。</p> <p>Packaged CCE は特定の Active Directory 機能レベルを必要としません。</p>
Microsoft SQL Server 2008 R2 x64 Standard Edition	Service Pack 2	Unified CCE データ サーバに使用されます。
アンチウイルス	<p>次のいずれかになります。</p> <ul style="list-style-type: none"> • Symantec Endpoint Protection 12.1 • Trend Micro Server Protect バージョン 5.8 • McAfee VirusScan Enterprise 8.8i 	Windows プラットフォームで実行されるすべてのアプリケーションに必要です。

ソフトウェアライセンス

ソフトウェアライセンスまたはPAK	数量	Packaged CCE ライセンス SKU に含まれているか	必須かどうか	詳細
Unified CVP	4つのPAK	Yes	Yes	4つの必要な Unified CVP Call/VXML サーバごとに1つのPAK
Unified Intelligence Center	1つのPAK	Yes	Yes	A側の Unified Intelligence Center パブリッシャに適用する1つのPAK
Unified Call Studio	2つのPAK	Yes	Yes	各 Unified Call Studio ワークステーションに1つのPAK。
Unified CVP Reporting Server	1つまたは2つのPAK	No	No	各オプション Unified CVP Reporting Server につき最大2つの追加の Unified CVP PAK。
Microsoft Windows Server 2008 R2	9-10ライセンス	No	Yes	<p>必要な Unified CCE コールおよびデータ サーバごとに1つの仮想 OS ライセンス = 4 ライセンス。</p> <p>必要な4つの Unified CVP コール/VXML サーバごとに1つの仮想 OS ライセンス = 4 ライセンス。</p> <p>Unified CVP OAMP サーバに1つの仮想 OS ライセンス = 1 ライセンス。</p> <p>オプションの Unified CVP Reporting サーバに1つの追加 Windows Server 仮想 OS ライセンス。</p> <p>(注) Microsoft Windows Server ライセンス オプションの詳細については、Microsoft または Microsoft の認定リセラーにお問い合わせください。</p>
Microsoft SQL Server 2008	2ライセンス	No	Yes	各データ サーバに1ライセンス。
VMware vSphere Standard または Enterprise ESXi 5.x	4ライセンス	No	Yes	<p>A側のサーバに2ライセンス、B側のサーバに2ライセンス。</p> <p>各サーバの CPU ごとに1ライセンス。各サーバには CPU が2つあります。</p>

ソフトウェアライセンスまたはPAK	数量	Packaged CCE ライセンス SKU に含まれているか	必須かどうか	詳細
VMware vCenter 5.x	1 ライセンス	No	No	Packaged CCE ゴールデンテンプレートの複製プロセスを使用するパートナーに必要です。 VMware vCenter のバージョンが管理される vSphere ESXi ホストのバージョン以降である必要があります。

サポートされるブラウザ

次のブラウザは、リリース 10.5 でサポートされています。

- Microsoft Internet Explorer 9 および 11
- Mozilla Firefox 24 以降



第 2 章

カスタマー サイト サーバの準備

このセクションのすべての手順を A 側と B 側のサーバで実行します。

- [Cisco USC C シリーズ カスタマー サイト サーバの準備, 11 ページ](#)
- [Cisco UCS B シリーズ カスタマー サイト サーバの準備, 15 ページ](#)
- [NTP および時刻同期, 21 ページ](#)

Cisco USC C シリーズ カスタマー サイト サーバの準備

C240 MS3 TRC#1 の RAID の設定

この手順を使用して作成される各アレイに対して、次の設定値を使用します。

- [ストライプ サイズ (Stripe size)] : [128KB]
- [読み取りポリシー (Read Policy)] : [常に先読み (Read Ahead Always)]
- [書き込みポリシー (Write Policy)] : [ライトバック (BBU) (Write Back with BBU)]

手順

- ステップ 1** サーバの電源を投入し、Quiet Boot が BIOS で無効になっていることを確認します。
- ステップ 2** 初期の起動シーケンス中に [Ctrl+H] キーを押して、MegaRAID BIOS 設定ユーティリティを入力します。
- ステップ 3** [開始 (Start)] をクリックします。
- ステップ 4** 左側のパネルで [設定ウィザード (Configuration Wizard)] を選択します。 [新規設定 (New Configuration)] をクリックします。次に、[次へ (Next)] をクリックします。
- ステップ 5** 設定をクリアするプロンプトで、[はい (Yes)] をクリックします。
- ステップ 6** [手動設定 (Manual Configuration)] を選択します。次に、[次へ (Next)] をクリックします。
- ステップ 7** 次の画面の左側のパネルで、最初の 8 つのドライブを追加して、次のようにドライブ グループ 0 を作成します。
- ドライブ 1 ~ 8 を選択します。
 - [アレイに追加 (Add to Array)] をクリックします。
 - [DG の受け入れ (Accept DG)] をクリックします。
- ステップ 8** 残りの 8 つのドライブを追加して、次のようにドライブ グループ 1 を作成します。
- 左側のパネルで、ドライブ 9 ~ 16 を選択します。
 - [アレイに追加 (Add to Array)] をクリックします。
 - [DG の受け入れ (Accept DG)] をクリックします。
 - [次へ (Next)] をクリックして、ドライブ グループを受け入れます。
- ステップ 9** 次のように、ドライブ グループ 0 をスパンに追加します。
- [ドライブ グループ 0 (Drive Group0)] を選択します。
 - [スパンに追加 (Add to Span)] をクリックします。
 - [次へ (Next)] をクリックします。
- ステップ 10** 次のように、Drive Group0 に対して RAID を設定します。
- [RAID レベル (RAID Level)] の場合、[RAID 5] を選択します。
 - [ストライプ サイズ (Stripe Size)] の場合、[128KB] を選択します。
 - [読み取りポリシー (Read Policy)] の場合、[read ahead = always] を選択します。
 - [書き込みポリシー (Write Policy)] の場合、[ライトバック (BBU) (write back with bbu)] を選択します。
 - [サイズの更新 (Update Size)] をクリックして、RAID のボリュームを最終決定し、結果として生成されるボリュームのサイズを確認します。1.903TB になります。
 - [受け入れ (Accept)] をクリックして、仮想ドライブの定義の VD0 を受け入れます。
 - [次へ (Next)] をクリックします。
 - [戻る (Back)] をクリックして、2 つめの RAID 5 アレイを追加します。
- ステップ 11** [戻る (Back)] をクリックして、次のように 2 つめの RAID 5 アレイを追加します。
- [デバイス グループ 1 (Drive Group1)] を選択します。
 - [スパンに追加 (Add to Span)] をクリックします。

c) [次へ (Next)] をクリックします。

ステップ 12 RAID 選択画面で、次の手順を実行します。

a) [RAID レベル (RAID Level)] の場合、[RAID 5] を選択します。

b) [ストライプ サイズ (Stripe Size)] の場合、[128KB] を選択します。

c) [読み取りポリシー (Read Policy)] の場合、[read ahead = always] を選択します。

d) [書き込みポリシー (Write Policy)] の場合、[ライトバック (BBU) (write back with bbu)] を選択します。

e) [サイズの更新 (Update Size)] をクリックします。サイズは 1.903TB になります。

f) [受け入れ (Accept)] をクリックして、仮想ドライブの定義の VD1 を受け入れます。

ステップ 13 BBU 警告画面で [はい (Yes)] をクリックします。

ステップ 14 [Virtual Live Definition] 画面で [次へ (Next)] をクリックして、仮想ドライブの定義が終了したことを通知します。

ステップ 15 [設定プレビュー (Configuration Preview)] 画面で [受け入れ (Accept)] をクリックして、RAID 設定を受け入れます。

ステップ 16 [はい (Yes)] をクリックして設定を保存します。

ステップ 17 [はい (Yes)] をクリックしてドライブの設定を開始します。

ステップ 18 両方のドライブのステータスが [最適化済み (Optimal)] と表示されたら、[ホーム (Home)] をクリックして、ウィザードを終了します。

ステップ 19 [終了 (Exit)] をクリックします。

ドライブの RAID 設定が完了すると、システムは新しい RAID アレイの初期化 (フォーマット) を試みます。これが開始されると、初期化の最新状況が Web BIOS 画面から確認できます。このバックグラウンドでの初期化が完了するのを待ったうえで、ESXi のインストールなど、後続のサーバ設定手順に進んでください。

Web BIOS の [Home] 画面または [仮想ドライブ (Virtual Drives)] 画面のバックグラウンド初期化の進行状況を確認できます。

VMware vSphere ESXi のインストール

Packaged CCE は、インストールしている Packaged CCE のリリースでサポートされる特定のバージョンの VMware マニュアル ([VMware サイト](#)) で検索可能な標準のインストール手順を使用します。

Packaged CCE では、ESXi をサーバのデフォルトのブートドライブとして最初のドライブにインストールする必要があること以外の固有の要件がありません。

vCenter へのカスタマー ESXi ホストの追加

<https://www.vmware.com/support/pubs/> で、vCenter サーバおよびホスト管理のマニュアルを参照してください。



(注) vCenter は、ゴールデンテンプレートにのみ必要です。

vCenter を使用していないお客様は管理デスクトップにインストールして、Packaged CCE サーバを管理できます。

RAID Config Validator ユーティリティの実行

RAID 設定をセットアップした後、このユーティリティを実行して、データストア設定を正しい状態にします。

手順

ステップ 1 <http://software.cisco.com/download/type.html?mdfid=284360381&i=rm> の [Packaged CCE Download Software] > [Deployment Scripts] ページから Packaged CCE RAID Config Validator ユーティリティをダウンロードします。

このユーティリティは、Java jre または jdk バージョン 1.6 がインストールされたコンピュータ上でローカルに抽出し、実行できる zip ファイルです。

ステップ 2 Windows コマンドプロンプトを開き、ファイルをダウンロードしたディレクトリに変更します。次に、**java -jar PackagedCCEraidConfigValidator-10.5.jar <IP Address of the Side A server> <username> <password>** コマンドを入力して、ツールを実行します。

次に例を示します。

```
C:\Users\Administrator\Desktop>java -jar PackagedCCEraidConfigValidator-10.5.jar xx.xx.xxx.xxx
  userName password
```

検証が開始していることを示すメッセージがモニタに表示されます。

有効または無効の設定のインジケータが表示されます。

一部のエラーの内容は、次のとおりです。

- サポート対象でないサーバが検出されました。または使用されています。
- 誤った数のデータストアが検出されました。
- データストアに設定されたサイズが正しくありません。

ステップ 3 ステップ 3 の B 側サーバの IP アドレスを入力して、ステップ 2 を繰り返し行ってください。

次の作業

ユーティリティが無効の設定を報告する場合、RAID 構成を再作成する必要があります。これには、RAID 構成をリセットし、ESXi を再びインストールし、RAID Config Validator ユーティリティを再実行して、設定を再検証する必要があります。

Cisco UCS B シリーズ カスタマー サイト サーバの準備

この項での設定手順は、カスタマーサイト UCS B シリーズがインストールされ、設定され、運用されていることが前提です。

UCS B シリーズのインストールおよび設定の詳細およびガイダンスについては、UCS B シリーズのマニュアル (<http://www.cisco.com/c/en/us/products/servers-unified-computing/product-listing.html>) または Cisco Data Center Unified Computing で Authorized Technology Provider を参照してください。

この項では、UCS B シリーズ プラットフォームに Packaged CCE を展開する場合での、特定の設定要件のみを説明します。顧客には、データセンターの要件とインフラストラクチャに応じて、多様な設計と設定が必要になる場合があります。ただし、どの設定でも、高可用性についての Packaged CCE の要件を満たす必要があります。たとえば、設計では、単一点障害を発生させる可能性を排除する必要があります。これは、シスコのコール処理アプリケーションの運用に悪影響を及ぼす場合があるためです。

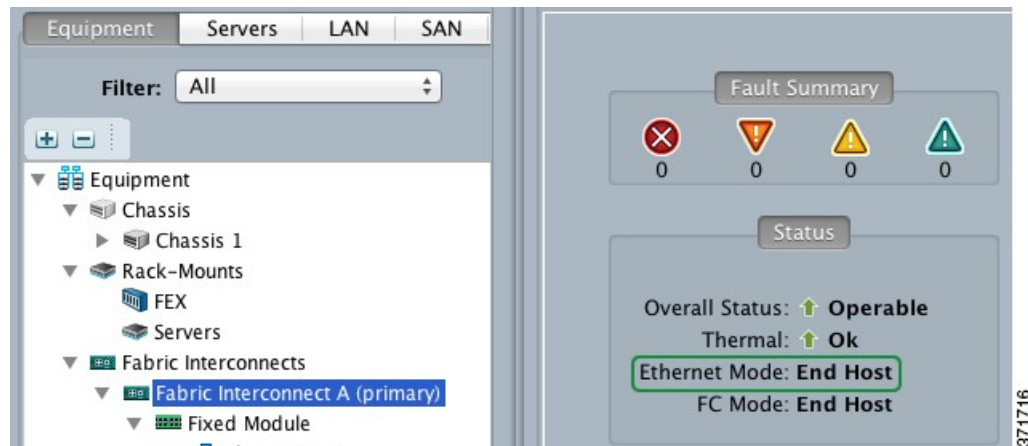


(注) この項での UCS ハードウェアのすべての構成例は、Cisco UCS Manager GUI を使用しています。UCS Manager CLI または API を使用する場合があります。

ファブリック インターコネクトの要件

Ethernet Mode

ファブリック インターコネクトのイーサネット モードは、エンドホストに設定する必要があります。



イーサネット アップリンク

Packaged CCE 用の Cisco UCS ファブリック インターコネクト イーサネット アップリンク (アップリンク ポート) は、2つの Common-L2 のデータセンター スイッチに相互接続されたそれぞれのファブリック インターコネクトで、10G にする必要があります。アップリンクは、単一リンク、ポート チャンネル (EtherChannel)、vPC、または VSS (MEC) アップリンク トポロジ内に存在する可能性があります。

ポート チャンネル アップリンクが使用される場合、UCS Manager で対応するポート チャンネルを作成する必要があります。この場合、そのポート チャンネルの ID をデータセンター スイッチでの ID と一致させるようにします。

データセンター スイッチへのポート チャンネル アップリンクが使用される場合、UCS B シリーズ ファブリック インターコネクトは Link Aggregation Control Protocol (LACP) のみをサポートします。データセンター スイッチとポート チャンネルが、LACP 用に設定されていることを確認してください。この要件は、vPC と VSS のポート チャンネルにも適用されます。

FC モード

エンドホストとスイッチング モードはどちらもサポートされています。サポートされる FC スイッチを備えた FC と FCoE NPIV には、エンドホストがデフォルトです。ファブリック インターコネクトで設定されるには、スイッチング モードでは FC ゾーン分割が必要です。これらのモードと使用例の詳細については UCS ファブリック インターコネクトのマニュアルを参照してください。また、必要に応じて、特定の SAN スイッチおよび SAN コントローラのベンダーのマニュアルを参照してください。UCS ファブリック インターコネクトのマニュアルは、次で入手することができます：<http://www.cisco.com/c/en/us/products/servers-unified-computing/ucs-6200-series-fabric-interconnects/index.html>。

FC ストレージ ポートおよび FCoE アップリンク

Packaged CCE は、ストレージの冗長性、遅延、IO、帯域幅の要件がすべて満たされることを前提として、UCS ファブリック インターコネクトでサポートされているように、SAN トポロジを接続したすべての FC および FCoE サポートしています。



(注)

SAN を直接接続で使用する場合、FC と FCoE の直接接続が認定されているストレージベンダーは、EMC、日立データシステムズ、NetApp に現在限定されています。認定された最新のベンダーとモデルについては、Cisco UCS ハードウェアの最新の互換性リストを参照してください：http://www.cisco.com/en/US/products/ps10477/prod_technical_reference_list.html。

QoS システム クラスと QoS ポリシー

Unified CM と CCE アプリケーションは L3 QoS DSCP (AF/CS) を設定しますが、ファブリック インターコネクトはそれを扱いません。ファブリック インターコネクトは、L3 を認識しないためです。Packaged CCE では、VMware vSwitch に対して、特定の QoS システム クラスまたは QoS ポリシーを設定する必要はありません。

関連トピック

[Cisco UCS B シリーズ サーバのネットワーク要件, \(29 ページ\)](#)

Cisco UCS B シリーズ ブレードの要件

Cisco UCS Manager はプール、ポリシー、およびテンプレートを使用します。これらは、サービスプロファイルテンプレートに収集され、サービスプロファイルとしてブレードに適用されます。

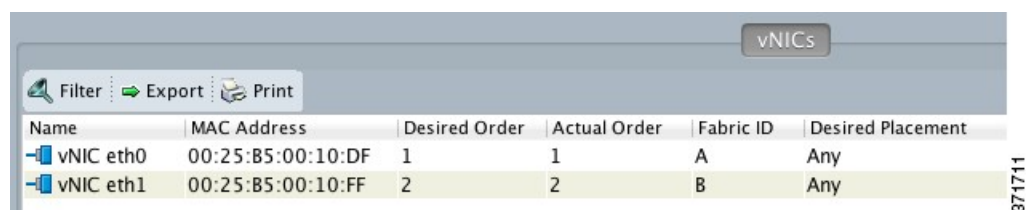
Packaged CCE には、ネットワーク VLAN と FC/FCoE VSAN の要件に適合させるための vNIC と vHBA の要件はありますが、ブレードのサービスプロファイルまたはサービスプロファイルテンプレートに対する具体的な要件はありません (vNIC の要件, (17 ページ) および vHBA の要件, (18 ページ) を参照)。

設定の一貫性と検証可能性、およびサーバの設定の準拠を確保するには、vNIC、vHBA、およびサービスプロファイルテンプレートを使用します。

UCS ブレード設定やサービスプロファイルとテンプレートの詳細については、該当する Cisco UCS Manager のマニュアルを参照してください。

vNIC の要件

Packaged CCE では、UCS B シリーズ ブレードで 2 つ以上の vNIC イーサネットインターフェイスを設定する必要があります。冗長性を確保するために、これら 2 つのインターフェイスを、代替ファブリック インターコネクタにそれぞれ割り当てます。



Name	MAC Address	Desired Order	Actual Order	Fabric ID	Desired Placement
vNIC eth0	00:25:B5:00:10:DF	1	1	A	Any
vNIC eth1	00:25:B5:00:10:FF	2	2	B	Any

Packaged CCE ホストのどの vNIC インターフェイスにも、ファブリック フェールオーバーは有効にしないでください。



Properties

Name: eth0

Description:

Owner: Local

Fabric ID: Fabric A Fabric B Enable Failover

VMware VMKernel と管理インターフェイスでは、Packaged CCE と同じ vNIC を共有できます。この表は、すべての VLAN で使用できなくなった vNIC インターフェイスの例です。

vNIC	VLANS	ファブリック	注意
eth0	PCCE 可表示 (アクティブ) PCCE プライベート (スタンバイ) VMware Kernel と管理 (アクティブ) デフォルトの VLAN (アクティブ) その他の管理 (アクティブ)	A	アクティブとスタンバイは、ファブリック インターコネクタに配置され、VMware 層で制御される状況で、これらの vNIC を経由するトラフィック フローのリファレンス設計を示す用語です。詳細については、UCS B シリーズの「ネットワーキング」の項を参照してください。
eth1	PCCE 可表示 (スタンバイ) PCCE プライベート (アクティブ) VMware Kernel と管理 (スタンバイ) デフォルトの VLAN (スタンバイ) その他の管理 (スタンバイ)	B	



(注) Packaged CCE の可表示ネットワークとプライベート ネットワーク以外のネットワークは、表に示されているように、アクティブ/スタンバイに設定する必要はありません。これらはアクティブ/アクティブ (上書きなし) に設定することができます。または必要に応じて、インフラストラクチャに全体に負荷を均等に分散するように割り当てることができます。

vHBA の要件

UCS B シリーズ ブレードでは、2 つ以上の vHBA FC インターフェイスを設定する必要があります。冗長性を確保するために、これら 2 つのインターフェイスを、代替ファブリック インターコネクタにそれぞれ割り当てます。

Name	WWPN	Desired Order	Actual Order	Fabric ID	Desired Placement
vHBA fc1	20:00:00:25:B5:00:10:DF	4	4	B	Any
vHBA fc0	20:00:00:25:B5:00:10:EF	3	3	A	Any

これらの FC vHBA は、FC または FCoE のいずれかに接続された SAN に使用できます。Cisco UCS のベストプラクティスは、共通 VSAN もサポートされていますが、ファブリック インターコネクタ (A/B) の SAN へのパスごとに、別の VSAN を使用することです。

共通 (図に示す) または別の vHBA インターフェイスは、SAN ストレージパスから Packaged CCE データストアと ESXi の起動に使用される場合があります。

SAN プロビジョニング用の Packaged CCE アプリケーション IOPS

この項では、Storage Area Networks (SAN) のプロビジョニングに使用する、Packaged CCE アプリケーション IO の要件を詳しく説明します。これらのデータポイントを使用して、LUN に対して適切にサイジングとプロビジョニングを行う必要があります。適切に行うことで、vSphere のデータストアにマップされ、その後 Packaged CCE アプリケーションをホストできるようになります。パートナーと顧客は SAN ベンダーと緊密に協力して、これらの要件に合わせて LUN をサイジングしてください。

UCS B シリーズでの Packaged CCE には、LUN/データストアの固定した数、つまり定数は必要ありません。代わりに、顧客は、Packaged CCE アプリケーション IOPS のスループットと遅延の要件が満たされることを前提として、1つのみのマッピングを使用するか、アプリケーション VM から LUN への 1対1のマッピングを使用する場合があります。所定のどの LUN 設計でも、ベンダーや SAN モデルごとに違いがあります。ここで定められる要件を満たすために、SAN ベンダーと緊密に協力して、最適なソリューションを判断してください。

このトピックに記載された IOPS は、Packaged CCE のオンボックス コンポーネントに限定したものです。オンボックス以外のアプリケーションの IOPS 要件については、各アプリケーションのマニュアルを参照してください。

表 1: 最大 1000 エージェントに対する IOPS

Packaged CCE コンポーネント	95th Pct	Average	Peak	Read %	Write %
Unified CCE コール サーバ	54	49	100	1	99
Unified CCE データ サーバ	481	388	4468	1	99
Unified CVP Server	6	4	95	5	95
Finesse Server	26	21	375	1	99
Unified CVP OAMP Server	5	4	48	1	99
Unified Intelligence Center	210	196	507	1	99

Packaged CCE コンポーネント	95th Pct	Average	Peak	Read %	Write %
Unified Communications Manager パブリッシャ	27	25	271	1	99
Unified Communications Manager サブスクリバ	36	32	446	1	99
Unified CVP Reporting Server	44	9	217	5	95

表 2: 最大 1000 エージェントに対する KBps

Packaged CCE コンポーネント	95th Pct	Average	Peak	Read %	Write %
Unified CCE コール サーバ	2656	2211	3252	1	99
Unified CCE データ サーバ	2654	2269	549986	19	81
Unified CVP Server	176	171	37016	5	95
Finesse Server	1278	977	5108	1	99
Unified CVP OAMP Server	38	46	28564	1	99
Unified Intelligence Center	1185	1091	2818	1	99
Unified Communications Manager パブリッシャ	333	264	3205	1	99
Unified Communications Manager サブスクリバ	653	568	3451	1	99
Unified CVP Reporting Server	820	175	42483	5	95



(注)

- 95th Pct、Average、Peak の所定の値は、Read と Write の合計です。
- 要件は、所定のアプリケーションのインスタンスあたりのものです。
- 複数の vDisk があるアプリケーション VM では、所定の総計値にそれらの複数のデバイスが加算されています。また、それらの要件を満たすために、それらのデバイスは、十分なリソースがある同じ LUN/Datastore で展開される必要があります。
- CVP Reporting Server の IOPS には、有効になったオン ボックス VXML レポートは含まれません。

SAN LUN プロビジョニングには、次のようなの要件と制限があります。

o

- SAN LUN からの VMware vSphere のブートは、Packaged CCE アプリケーション VM と共有されない場合があります。SAN からのブートについては、VMware と SAN ベンダーのベストプラクティスを参照してください。
- シンプロビジョニングされた LUN はサポートされています。これらは、すべての Packaged CCE アプリケーション VM で必要となる全スペースを収納できるような、十分なスペースで起動する必要があります。これは、これらの VM vDisk がシンプロビジョニングをサポートしていないためです。
- SAN では、データの重複排除はサポートされません。
- 作成された LUN を収納する際に使用される SAN ディスク アレイには、RAID 0 または RAID 1 はサポートされません。RAID 0 は冗長性を備えておらず、RAID 1 はアプリケーションのパフォーマンスに悪影響を及ぼします。

RAID レベル 5、6、10 が最も一般的です。SAN ベンダーが提供するその他の高度な RAID レベルは、アプリケーションの IOPS、スループット、遅延の要件が満たされることを前提として、サポートされています。
- 階層型ストレージがサポートされています。
- SAN で Packaged CCE を使用する場合、7200 RPM とそれ以下の低速なドライブは、不十分な遅延によりサポートされていません。この要件の例外は、そのドライブが階層型ストレージプールで使用されており、同じプールに 10,000/15,000 RPM ドライブや SSD 階層を備えている場合です。

NTP および時刻同期

Packaged CCE では、ソリューションのすべての部分と同じ時刻に設定されている必要があります。時間のずれは自然に発生しますが、ソリューションコンポーネントの同期を維持するために NTP を設定することは重要です。

ライブ データ レポートの時間のずれを回避するには、データ サーバ VM の NTP 設定、コール サーバの VM、および Cisco Unified Intelligence Center パブリッシャとサブスクライバの VM が同期されている必要があります。

Cisco UCS B シリーズサーバの場合、UCS Manager を使用して、タイムゾーンと NTP タイムサーバを設定する必要があります。詳細については、「[Cisco UCS B シリーズサーバのタイムゾーンと NTP タイムサーバの設定](#)、(23 ページ)」を参照してください。

Windows Active Directory ドメイン

Packaged CCE ドメインが常駐する（同じであるか、親またはピア）フォレストの Windows Active Directory PDC エミュレータ マスターが、外部時刻源を使用するように適切に設定されている必要があります。この外部時刻源は信頼できる確実な NTP プロバイダーである必要があります。お客様のフォレストにすでに設定されている場合は、Packaged CCE ソリューションのこのセクションに記載されているように、他のすべてのアプリケーションで同じ時刻源として使用されており、使用可能である必要があります。

NTP 外部時刻源の Windows Active Directory ドメインを適切に設定するには、次の参考資料を参照してください。

- 『[How to configure an authoritative time server in Windows Server](#)』。



(注) この記事の「Fix it for me」機能は使用しないでください。

- 『[AD DS: The PDC emulator master in this forest should be configured to correctly synchronize time from a valid time source](#)』

Microsoft Windows Server のドメインは、ハードウェア障害または別の方法で、PDC エミュレータマスターサーバが失われると、ドメインの権限のある内部時刻源を自動的に回復したり、内部時刻源のフェールオーバーを行いません。『[Time Service Configuration on the DCwith PDC Emulator FSMO Role](#)』の記事は、ドメインの権限のある内部時刻源になるように新しいターゲットサーバをさらに追加する必要性について補助的に説明します。また、別のドメインコントローラに対する PDC FSMO の役割の回復、確保、または再割り当ての手動による介入について説明します。

ドメインの Windows コンポーネント

ドメインの Windows ホストは、権限のある内部時刻源を持つ PDC エミュレータで、またはドメインフォレスト階層で同じように連結されて、PDF エミュレータと時間を同期するように自動的に設定されます。

ドメインにない Windows コンポーネント

ドメインに結合されていない Windows Server の NTP 時刻源を設定するには、次の手順を使用してください。

- 1 [コマンドプロンプト (Command Prompt)] ウィンドウで、次の行を入力して、Enter キーを押します。w32tm /config /manualpeerlist:PEERS /syncfromflags:MANUAL



(注) NTP サーバのカンマ区切りリストを使用して、ピアを置き換えます。

- 2 w32time サービスを再開します : net stop w32time && net start w32time。
- 3 ピアと w32time サービスを同期します : w32tm /resync。
- 4 次のサービス コントロール コマンドを使用して、サーバの再起動で w32time サービスが適切に起動していることを確認します : sc triggerinfo w32time start/networkon stop/networkoff。

ESXi ホスト

すべての Packaged CCE ESXi ホスト (任意のコンポーネントを含む) は、外部時刻源として Windows ドメイン PDC エミュレータ マスターによって使用される同じ NTP サーバを指している必要があります。

Cisco サービス統合型ルータ

Cisco IOS 音声ゲートウェイは、ログインおよびデバッグの正確な時間を提供するためにソリューションで同じ NTP ソースを使用するように設定する必要があります。『[Basic System Management Configuration Guide, Cisco IOS Release 15M&T: Setting Time and Calendar Services](#)』を参照してください。

VOS コンポーネント

Unified Intelligence Center、Finesse、Social Miner、および Unified Communications Manager などのコンポーネントは、ドメインの権限のある内部時刻源と同じ NTP サーバを指している必要があります。

NTP サーバの CLI コマンド

NTP サーバは通常、インストール時間に指定されていますが、ntp サーバを表示、追加、および削除する上記のコンポーネントのプラットフォーム CLI から使用できるいくつかのコマンドを示します。プラットフォーム CLI から、次の内容を実行します。

- 既存の ntp サーバを表示する場合 : `utils ntp servers list`
- 追加の NTP サーバを追加する場合 : `utils ntp server add <追加するホストまたは IP アドレス>`
- 既存の NTP サーバを削除する場合 : `utils ntp server delete (削除する項目の行番号) Enter` キーを押します。

Cisco UCS B シリーズ サーバのタイムゾーンと NTP タイムサーバの設定

UCS Manager で UCS B シリーズ サーバのタイムゾーンと NTP タイムサーバを設定します。

手順

-
- ステップ 1 UCS Manager の [Admin] タブで、[Stats Mangement] > [Time Zone Management] を選択します。
 - ステップ 2 ドロップダウンメニューから、[Time Zone] を選択します。
 - ステップ 3 [Add NTP Time Server] をクリックします。
 - ステップ 4 NTP タイムサーバの IP アドレスを入力し、[OK] をクリックします。
 - ステップ 5 [Save (保存)] をクリックします。
-



第 3 章

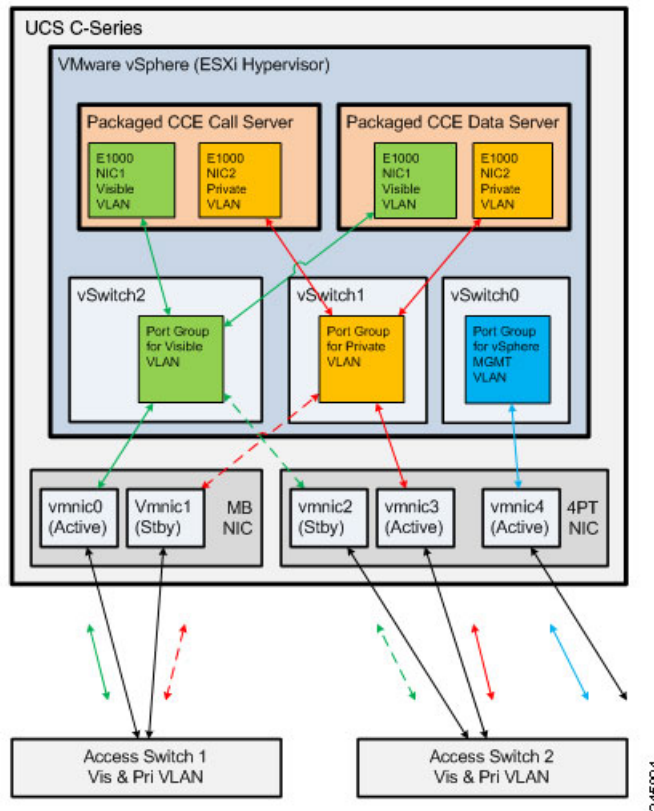
ネットワーク設計の考慮事項

この章では、UCS サーバに Packaged CCE を導入するために必要なネットワーク設定を実行するためのガイドラインを示します。また、耐障害性と冗長性の情報が含まれます。

- [Cisco UCS C シリーズ サーバのネットワーク要件, 25 ページ](#)
- [Cisco UCS B シリーズ サーバのネットワーク要件, 29 ページ](#)
- [帯域幅のプロビジョニングおよびネットワーク QoS の考慮事項, 40 ページ](#)

Cisco UCS C シリーズ サーバのネットワーク要件

図は、vSphere vSwitch 設計の UCS C シリーズ サーバおよびネットワーク実装のすべての Packaged CCE の展開で参照される設計を示します。



この設計では、ネットワークへの代替および冗長ハードウェアパスを介したアクティブ/スタンバイ構成の仮想マシンのネットワークインターフェイスコントローラ (vmnic) のVMware NIC チューミング (ロードバランシングなし) の使用を求めます。

ネットワーク側の実装はこの図に正確に一致させる必要はありませんが、冗長性を考慮し、表示およびプライベートネットワーク通信の両方に影響する単一点障害を回避する必要があります。



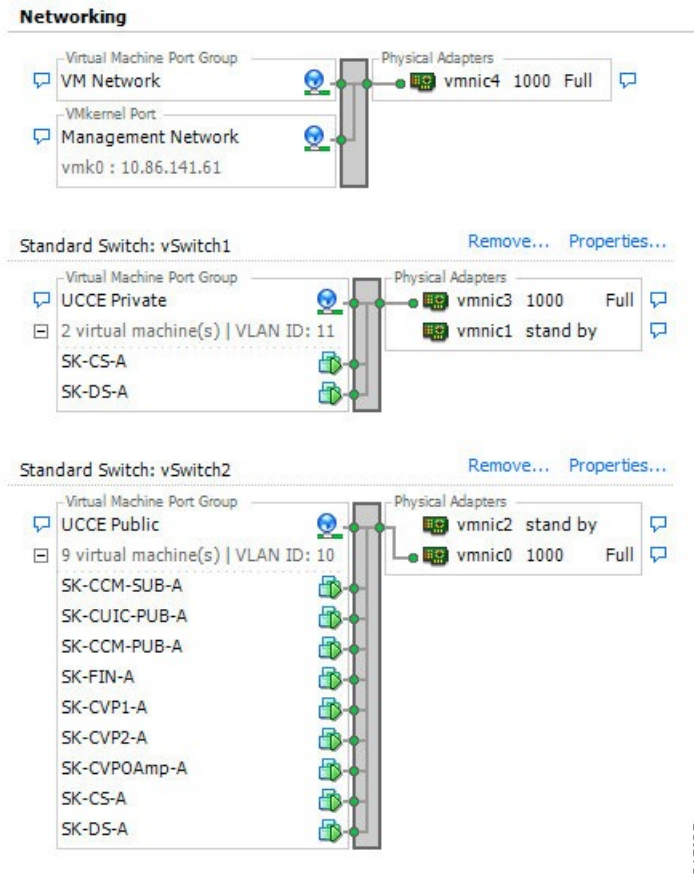
(注) お客様にはまた、各自の判断でデータセンターの同一または別個のスイッチインフラストラクチャ上の管理 vSwitch に VMware NIC チューミングを設定するオプションがあります。

要件：

- イーサネットインターフェイスは、ギガビット速度で、ギガビットイーサネットスイッチに接続されている必要があります。10/100 イーサネットはサポートされません。
- 表示およびプライベートネットワークで、単一点障害が存在しないようにします。
- ネットワークスイッチのインフラストラクチャは、Cisco Stacking テクノロジーを使用して、UCS C シリーズのサーバが単一の仮想スイッチに接続されている場所にすべてのスイッチを結合することはできません。
- ネットワークスイッチは、VMware への接続で適切に設定されている必要があります。フェールオーバー/フォールバックシナリオの Spanning Tree Protocol (STP) 遅延を防ぐための適切なスイッチの設定の詳細については、『[VMware Knowledge Base](#)』を参照してください。

Cisco UCS C シリーズ サーバ用の VMware vSwitch の設計

次の図は、冗長アクティブ/スタンバイの vSwitch NIC チューミング設計を使用した UCS C シリーズサーバの vSwitch と vmnic アダプタの設定について説明します。設定は、A 側サーバと B 側サーバで同じです。



UCS C シリーズ サーバイーサネット アップリンク用のデータセンタースイッチの設定

UCSC シリーズサーバ PackagedCCE の可表示ネットワークのイーサネットアップリンクのリファレンス設計および必須設計では、仮想スイッチ VLAN タギング (VST) モードと呼ばれる、IEEE 802.1Q (dot1q) トランキンングを使用します。この設計では、次の例で示すように、特定の設定がアップリンク データ センター スイッチで使用されている必要があります。

アップリンク ポートを不適切に設定すると、システムのパフォーマンス、操作、および障害処理に直接、悪影響を及ぼします。



(注) すべての VLAN 設定は、例を示すことを目的としています。顧客の VLAN は、特定のネットワーク要件に応じて異なる場合があります。

例：仮想スイッチ VLAN タギング

C3750-A1

```
interface GigabitEthernet1/0/1
  description PCCE_Visible_A_Active
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 10
  switchport mode trunk
  switchport nonegotiate
  spanning-tree portfast trunk

interface GigabitEthernet1/0/2
  description PCCE_Private_A_Standby
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 100
  switchport mode trunk
  switchport nonegotiate
  spanning-tree portfast trunk
```

C3750-A2

```
interface GigabitEthernet1/0/1
  description PCCE_Visible_A_Standby
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 10
  switchport mode trunk
  switchport nonegotiate
  spanning-tree portfast trunk

interface GigabitEthernet1/0/2
  description PCCE_Private_A_Active
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 100
  switchport mode trunk
  switchport nonegotiate
  spanning-tree portfast trunk
```

C3750-B1

```
interface GigabitEthernet1/0/1
  description PCCE_Visible_B_Active
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 20
  switchport mode trunk
  switchport nonegotiate
  spanning-tree portfast trunk

interface GigabitEthernet1/0/2
  description PCCE_Private_A_Standby
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 200
  switchport mode trunk
  switchport nonegotiate
  spanning-tree portfast trunk
```

C3750-B2

```
interface GigabitEthernet1/0/1
  description PCCE_Visible_B_Standby
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 20
```

```

switchport mode trunk
switchport nonegotiate
spanning-tree portfast trunk

interface GigabitEthernet1/0/2
description PCCE_Private_B_Active
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 200
switchport mode trunk
switchport nonegotiate
spanning-tree portfast trunk

```



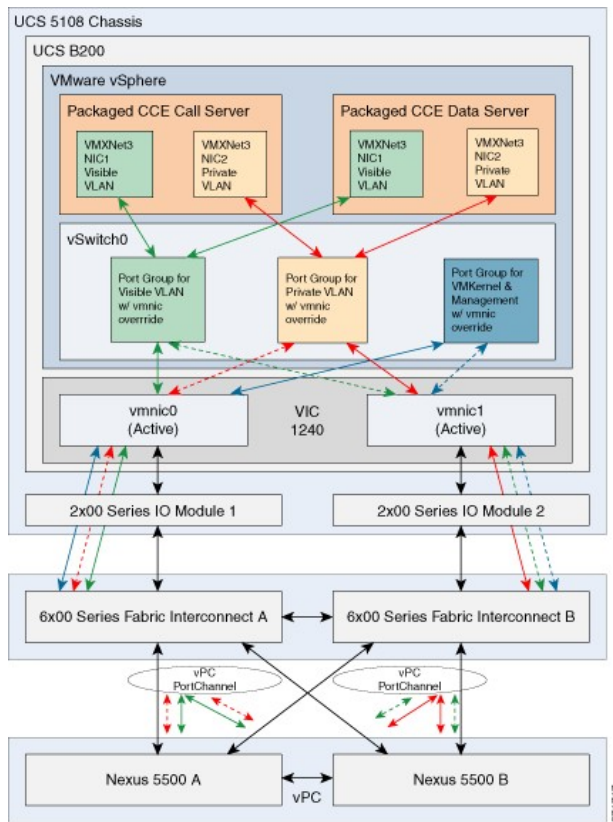
(注)

- ESXi は dot1q のみをサポートしています。
- DTP はサポートされません。

Cisco UCS B シリーズ サーバのネットワーク要件

以下の図では、アプリケーションのローカル OS NIC からデータセンター ネットワークのスイッチング インフラストラクチャへの、仮想的への Packaged CCE から物理的な Packaged CCE の通信パスを示します。

図に示す参照設計では、アクティブ/アクティブ モードで2つの vmnic を備えた単一の仮想スイッチを使用します。この設計には、VMware vSwitch のポート グループ vmnic オーバーライド機能を使用して、ファブリック インターコネク ト経由で調整された、多様な可表示ネットワークとプライベート ネットワークのパスがあります。

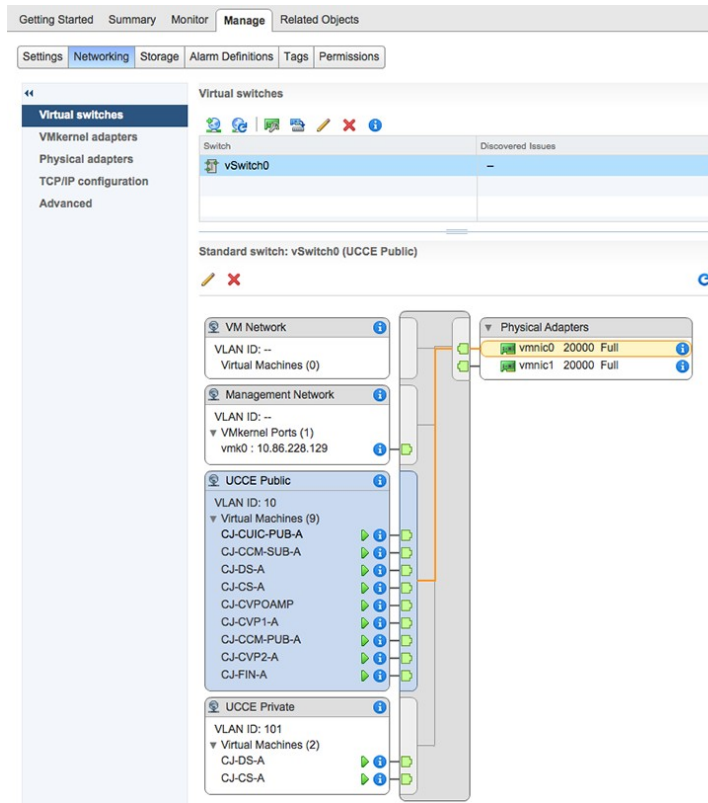


UCS C シリーズサーバでの設計と類似するような、別の設計も可能です。その設計では、各ポートグループ (VLAN) に、アクティブ/スタンバイの設定で2つの vmnic を備えた独自の vSwitch があります。どの設計でも、可表示ネットワークとプライベートネットワークのパスの多様性を維持する必要があり、どちらのネットワークでも、ファブリック インターコネクト経由で単一パスが損失する事態に陥らないようにします。

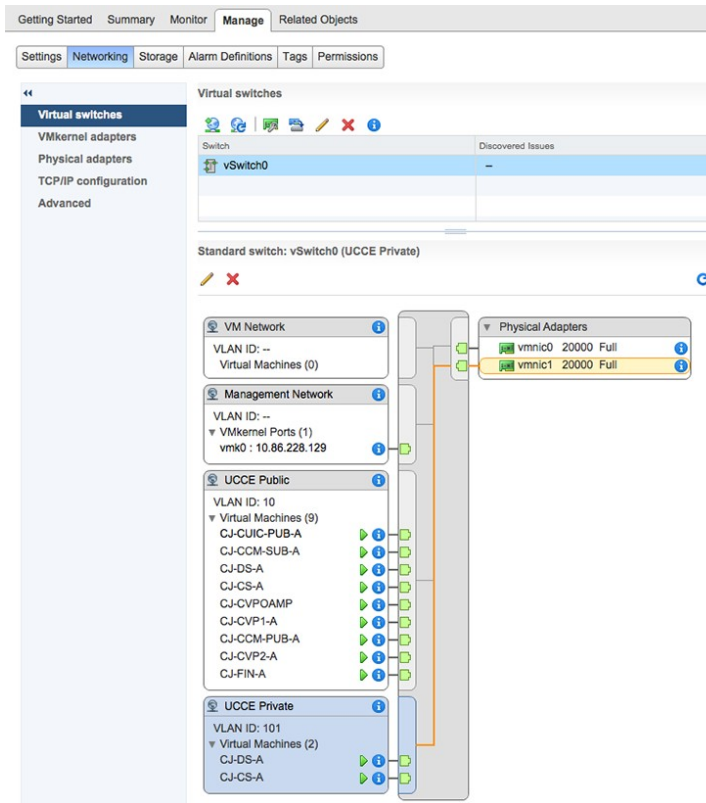
Cisco UCS B シリーズ サーバ用の VMware vSwitch の設計

このトピックの図では、UCS B シリーズ サーバ上の VMware vSwitch に対する、アクティブ/アクティブの vmnic チェーミング設計を使用した、ポートグループがある2つの vmnic インターフェイスのオーバーライドを示します。設定は、A 側サーバと B 側サーバで同じです。

次の図は、vmnic0 インターフェイスへのパブリックネットワークの配置 (オーバーライドでの優先パス) を示しています。

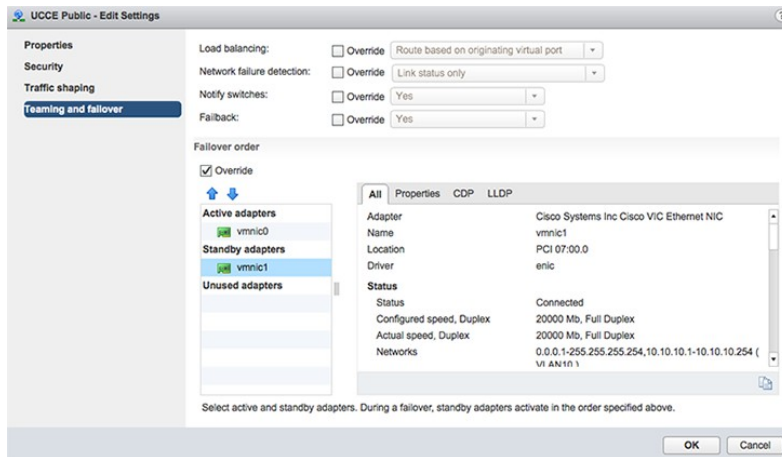


次の図は、vmnic1 インターフェイスへのプライベート ネットワークの配置を示しています。



371714

アクティブ/アクティブの vmnic インターフェイスを使用する場合、vSphere Web クライアントの [vSwitch Properties] ダイアログで、アクティブ/スタンバイをポートグループ (VLAN) ごとに設定できます。



371710

Packaged CCE の可表示ネットワークとプライベートネットワークでのアクティブとスタンバイの vmnic は、ファブリック インターコネクタにより切り替わり、単一パスの障害により両方のネットワークの通信パスが同時にフェールオーバーしないことを確認します。これを調べるには、vSphere での vmnic の MAC アドレスを、UCS Manager でブレードに割り当てられた MAC アドレ

スと比較して、ファブリック インターコネク트가どの vmnic に配置されたかを確定する必要があります。場合があります。

UCS B シリーズ サーバは、UCS C シリーズ サーバで使用される設計と同じように、vSwitch のアクティブ/スタンバイの別のペアで、6 以上の vmnic インターフェイスを持つように設計される場合もあります。この設計では、可表示ネットワークとプライベートネットワークのアクティブなパスが、2 つのファブリック インターコネク트가の間で切り替わることが必要です。

Cisco UCS B シリーズ ファブリック インターコネク트가イーサネット アップリンク用のデータ センター スイッチの設定

ここでは、UCS B シリーズ ファブリック インターコネク트가に接続する際の、データセンター スイッチのアップリンク ポートの設定例について説明します。

UCS B シリーズ ファブリック インターコネク트가から Packaged CCE のデータセンター スイッチにイーサネット アップリンクを設定する場合、サポートされている設計が複数あります。仮想スイッチ VLAN タギング以外にも、データセンター スイッチの機能により、EtherChannel / Link Aggregation Control Protocol (LACP) および仮想 PortChannel (vPC) がオプションとして必要になります。

UCS ファブリック インターコネク트가から、Packaged CCE の可表示ネットワークとプライベートネットワークにアップリンクする場合、必須で参考となる設計では Common-L2 の設計を使用します。この設計では、どちらの Packaged CCE VLAN でもデータセンター スイッチのペアにトランクされます。顧客は、同じリンクのその他の管理 (VMware など) と企業ネットワークをトランクすることを選択したり、Disjoint-L2 モデルを使用して、Packaged CCE からこれらのネットワークを切り離したりできます。ここでは Common-L2 モデルのみを使用しますが、どちらの設計もサポートされています。



(注) すべての VLAN、vPC、PortChannel ID、および設定は、例を示すことを目的としています。顧客の VLAN、ID、および vPC のタイミングと優先度の設定は、特定のネットワーク要件に応じて異なる場合があります。

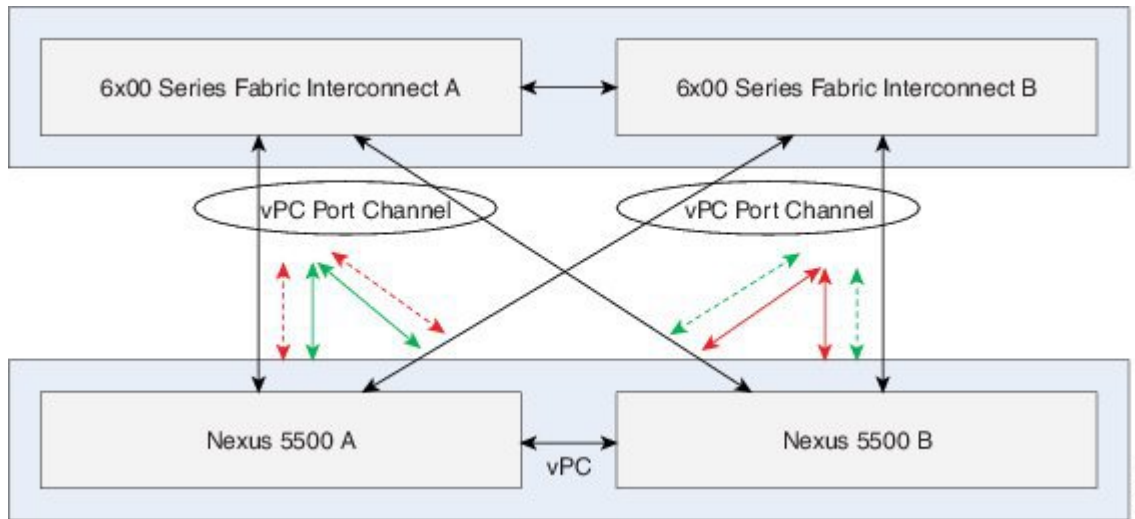
アップリンク ポートを不適切に設定すると、システムのパフォーマンス、操作、および障害処理に直接、悪影響を及ぼします。

例 1 : vPC のアップリンク

この例では、LACP と vPC を使用して、Cisco Nexus 5500 シリーズ スイッチのペアに、UCS ファブリック インターコネク트가イーサネットをアップリンクします。UCS ファブリック インターコネク��には LACP が必要です。ここでは、PortChannel アップリンクが、vPC かどうかにかかわらず、使用されます。



(注) VSS を備えた Cisco Catalyst 10G スイッチは、ファブリック インターコネク トへの VSS (MEC) アップリンクと同様のアップリンク トポロジで使用される場合もあります。IOS の設定はこ ここでは説明しません。IOS の設定は NX-OS の設定とは異なります。



N5KA

```

cfs ipv4 distribute
cfs eth distribute
feature lacp
feature vpc
feature lldp

vlan 1-10,100

vpc domain 1
  role priority 1000
  system-priority 4000
  peer-keepalive destination 10.0.0.2
  delay restore 180
  peer-gateway
  auto-recovery

interface port-channel1
  description vPC_to_FabricA
  switchport mode trunk
  switchport trunk allowed vlan 1-10,100
  spanning-tree port type edge trunk
  vpc 1

interface port-channel2
  description vPC_to_FabricB
  switchport mode trunk
  switchport trunk allowed vlan 1-10,100
  spanning-tree port type edge trunk
  vpc 2

interface port-channel100
  description vPC_Peer_Link
  switchport mode trunk
  spanning-tree port type network
  vpc peer-link
  
```

```

interface Ethernet1/1
  description Uplink-To-FabricA
  switchport mode trunk
  switchport trunk allowed vlan 1-10,100
  channel-group 1 mode active

interface Ethernet1/2
  description Uplink-To-FabricB
  switchport mode trunk
  switchport trunk allowed vlan 1-10,100
  channel-group 2 mode active

interface Ethernet1/5
  description Interswitch_Link
  switchport mode trunk
  channel-group 100

interface Ethernet1/6
  description Interswitch_Link
  switchport mode trunk
  channel-group 100

interface mgmt0
  ip address 10.0.0.1/24

no ip igmp snooping mrouter vpc-peer-link
vpc bind-vrf default vlan 4048

```

N5KB

```

cfs ipv4 distribute
cfs eth distribute
feature lacp
feature vpc
feature lldp

vlan 1-10,100

vpc domain 1
  role priority 2000
  system-priority 4000
  peer-keepalive destination 10.0.0.1
  delay restore 180
  peer-gateway
  auto-recovery

interface port-channel1
  description vPC_to_FabricA
  switchport mode trunk
  switchport trunk allowed vlan 1-10,100
  spanning-tree port type edge trunk
  vpc 1

interface port-channel2
  description vPC_to_FabricB
  switchport mode trunk
  switchport trunk allowed vlan 1-10,100
  spanning-tree port type edge trunk
  vpc 2

interface port-channel100
  description vPC_Peer_Link
  switchport mode trunk
  spanning-tree port type network
  vpc peer-link

interface Ethernet1/1
  description Uplink-To-FabricA
  switchport mode trunk
  switchport trunk allowed vlan 1-10,100
  channel-group 1 mode active

interface Ethernet1/2

```

```

description Uplink-To-FabricB
switchport mode trunk
switchport trunk allowed vlan 1-10,100
channel-group 2 mode active

interface Ethernet1/5
description Interswitch_Link
switchport mode trunk
channel-group 100

interface Ethernet1/6
description Interswitch_Link
switchport mode trunk
channel-group 100

interface mgmt0
ip address 10.0.0.2/24

no ip igmp snooping mrouter vpc-peer-link
vpc bind-vrf default vlan 4048

```



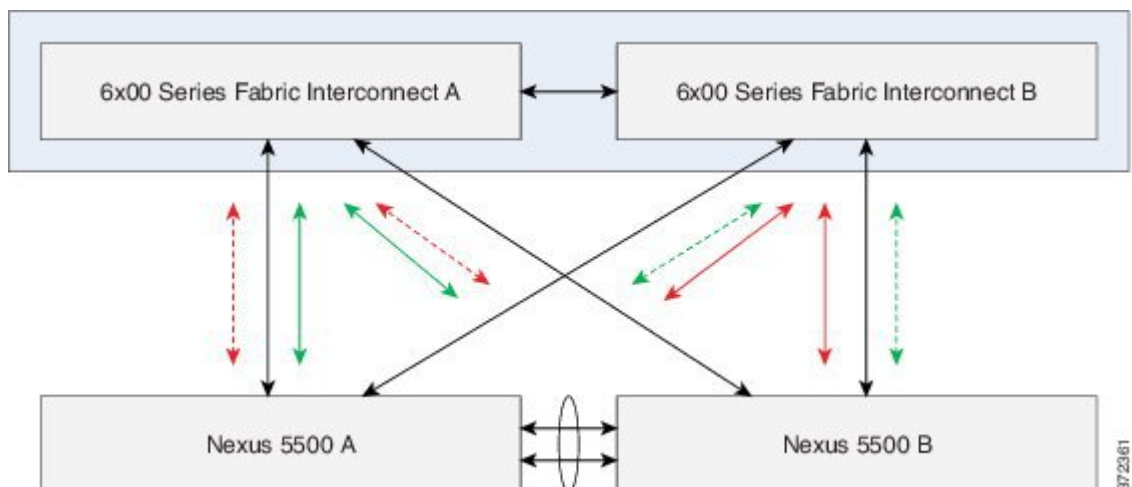
- (注) インターフェイスを vPC (チャンネルグループ) にさらに追加すれば、アップリンクの総帯域幅を増やすことができます。これらのインターフェイスは、両方の Nexus 5500 スイッチで対称的に追加する必要があります。

例 2 : 標準的なアップリンク

この例では、Cisco Nexus 5500 シリーズ スイッチのペアを、PortChannels と vPC なしで UCS ファブリック インターコネクต์にアップリンクしました (Nexus 5500 のペアは有効な vPC である場合があります)。



- (注) 10G イーサネットに対応した Cisco Catalyst スイッチは、同様のアップリンク トポロジを使用する場合があります。IOS の設定はここでは説明しません。IOS の設定は NX-OS の設定とは異なる場合があります。



```
N5KA
cfs ipv4 distribute
cfs eth distribute
feature lldp

vlan 1-10,100

interface port-channel100
  description L2-Interswitch-Trunk
  switchport mode trunk
  spanning-tree port type network

interface Ethernet1/1
  description Uplink-To-FabricA
  switchport mode trunk
  switchport trunk allowed vlan 1-10,100
  spanning-tree port type edge trunk

interface Ethernet1/2
  description Uplink-To-FabricB
  switchport mode trunk
  switchport trunk allowed vlan 1-10,100
  spanning-tree port type edge trunk

interface Ethernet1/5
  description Interswitch_Link
  switchport mode trunk
  channel-group 100

interface Ethernet1/6
  description Interswitch_Link
  switchport mode trunk
  channel-group 100
```

```
N5KB
cfs ipv4 distribute
cfs eth distribute
feature lldp

vlan 1-10,100

interface port-channel100
  description L2-Interswitch-Trunk
  switchport mode trunk
  spanning-tree port type network

interface Ethernet1/1
  description Uplink-To-FabricA
  switchport mode trunk
  switchport trunk allowed vlan 1-10,100
  spanning-tree port type edge trunk

interface Ethernet1/2
  description Uplink-To-FabricB
  switchport mode trunk
  switchport trunk allowed vlan 1-10,100
  spanning-tree port type edge trunk

interface Ethernet1/5
  description Interswitch_Link
  switchport mode trunk
  channel-group 100

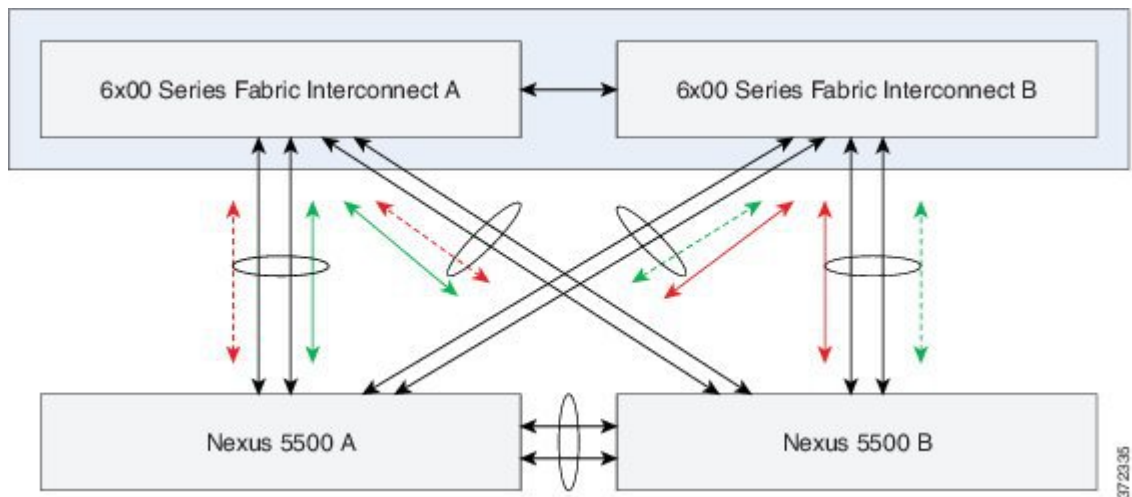
interface Ethernet1/6
  description Interswitch_Link
  switchport mode trunk
  channel-group 100
```

例 3 : EtherChannel のアップリンク

この例では、非 vPC PortChannel を備えた Nexus 5500 のペア（LACP を備えた EtherChannel）を、UCS ファブリック インターコネクต์にアップリンクします。



(注) 10G イーサネットに対応した Cisco Catalyst スイッチは、同様のアップリンク トポロジを使用する場合があります。IOS の設定はここでは説明しません。IOS の設定は NX-OS の設定とは異なる場合があります。

**N5KA**

```

cfs ipv4 distribute
cfs eth distribute
feature lacp
feature lldp

vlan 1-10,100

interface port-channel1
description PC_to_FabricA
switchport mode trunk
switchport trunk allowed vlan 1-10,100
spanning-tree port type edge trunk

interface port-channel2
description PC_to_FabricB
switchport mode trunk
switchport trunk allowed vlan 1-10,100
spanning-tree port type edge trunk

interface port-channel100
description Interswitch_Peer_Link
switchport mode trunk
spanning-tree port type network

interface Ethernet1/1
description Uplink-To-FabricA
switchport mode trunk
switchport trunk allowed vlan 1-10,100
channel-group 1 mode active

interface Ethernet1/2

```



```

description Uplink-To-FabricA
switchport mode trunk
switchport trunk allowed vlan 1-10,100
channel-group 1 mode active

interface Ethernet1/3
description Uplink-To-FabricB
switchport mode trunk
switchport trunk allowed vlan 1-10,100
channel-group 2 mode active

interface Ethernet1/4
description Uplink-To-FabricB
switchport mode trunk
switchport trunk allowed vlan 1-10,100
channel-group 2 mode active

interface Ethernet1/5
description Interswitch_Link
switchport mode trunk
channel-group 100

interface Ethernet1/6
description Interswitch_Link
switchport mode trunk
channel-group 100

```

N5KB

```

cfs ipv4 distribute
cfs eth distribute
feature lacp
feature lldp

vlan 1-10,100

interface port-channel1
description PC_to_FabricA
switchport mode trunk
switchport trunk allowed vlan 1-10,100
spanning-tree port type edge trunk

interface port-channel2
description vPC_to_FabricB
switchport mode trunk
switchport trunk allowed vlan 1-10,100
spanning-tree port type edge trunk

interface port-channel100
description PC_Peer_Link
switchport mode trunk
spanning-tree port type network

interface Ethernet1/1
description Uplink-To-FabricA
switchport mode trunk
switchport trunk allowed vlan 1-10,100
channel-group 1 mode active

interface Ethernet1/2
description Uplink-To-FabricA
switchport mode trunk
switchport trunk allowed vlan 1-10,100
channel-group 1 mode active

interface Ethernet1/3
description Uplink-To-FabricB
switchport mode trunk
switchport trunk allowed vlan 1-10,100
channel-group 2 mode active

interface Ethernet1/4
description Uplink-To-FabricB

```

```
switchport mode trunk
switchport trunk allowed vlan 1-10,100
channel-group 2 mode active

interface Ethernet1/5
description Interswitch_Link
switchport mode trunk
channel-group 100

interface Ethernet1/6
description Interswitch_Link
switchport mode trunk
channel-group 100
```

帯域幅のプロビジョニングおよびネットワーク QoS の考慮事項

ワイドエリアネットワークが QoS をサポートしている必要があります。詳細については、『*Cisco Unified Contact Center Enterprise Design Guide*』の「*Bandwidth Provisioning and QoS considerations*」を参照してください。http://www.cisco.com/en/US/partner/products/sw/custcosw/ps1844/products_implementation_design_guides_list.html



第 **II** 部

インストール：ゴールデン テンプレートと 直接インストール

- [インストール シナリオ, 41 ページ](#)
- [ゴールデン テンプレートの作成, 43 ページ](#)
- [カスタマー サイトでのゴールデン テンプレートの展開, 49 ページ](#)
- [ゴールデン テンプレートのインポート後, 61 ページ](#)
- [直接インストール, 75 ページ](#)
- [ゴールデン テンプレートと直接インストール用の共通タスク, 83 ページ](#)
- [ゴールデン テンプレートと直接インストール用のソフトウェア インストール, 89 ページ](#)

インストール シナリオ

インストールのシナリオ

Packaged CCE の展開では、2つのオプションがパートナーとサービス プロバイダーに提供されます。

- **ゴールデン テンプレートの作成**：後で任意の数のお客様向けに仮想マシン（VM）に複製およびインストールできるシスコ コンタクト センター アプリケーションの再利用可能なマスター コピーです。
- **直接インストール**：VM としてカスタマー サーバでシスコ コンタクト センター アプリケーションを直接展開できます。

インストール ワークフロー

シーケンス	タスク	参照先
1	必要なソフトウェア、ハードウェア、およびライセンスが揃っていることの確認	第 1 章
2	ゴールデン テンプレートの作成とエクスポート用の処理	第 2 章
または		
2	仮想マシンの直接作成	第 3 章
次に		
3	お客様向けのサーバの設定およびステージング	第 5 章 ~ 第 11 章
6	カスタマー サイトでの動作の確認。基本設定の実行、展開タイプの設定、およびコールの実行。	第 12 章 ~ 第 15 章

関連トピック

[ゴールデン テンプレートについて, \(43 ページ\)](#)

[直接インストールについて, \(75 ページ\)](#)



第 4 章

ゴールデン テンプレートの作成

- [ゴールデンテンプレートについて, 43 ページ](#)
- [ゴールデンテンプレートの作成, 44 ページ](#)

ゴールデン テンプレートについて

この章では、Packaged CCE の 2 つのインストールのシナリオのうち 1 つを説明します。ラボのシスコのコンタクトセンターアプリケーションにゴールデンテンプレートを作成し、それをカスタマーサイトにエクスポートします。



(注) もう一方のシナリオは、カスタマーサイトで仮想マシンを直接インストールします。ゴールデンテンプレートを作成する予定がない場合は、この章を省略して、第3章：[直接インストール, \(75 ページ\)](#)に進みます。

ゴールデンテンプレートは、多数のお客様が再利用できるコンタクトセンターアプリケーションのマスターコピーです。ゴールデンテンプレートを作成すると、複製可能な一連の基本インストールとコアアプリケーションの設定が容易されます。次に、カスタマーサイトでそれらをインポートし、お客様用にカスタマイズします。

これらは、ソースシステム上に作成され、パートナーまたはサービスプロバイダーによって制御されるサーバです。ゴールデンテンプレートが作成されたら、カスタマーサイトのペアの宛先サーバに仮想マシン (VM) として、展開用のゴールデンテンプレートを処理します。

次の手順で行います。

- 1 OVA ファイルをダウンロードします。 [Open Virtualization ファイル, \(83 ページ\)](#) を参照してください。
- 2 ESXi host フォルダの下フォルダに直接ゴールデンテンプレートを作成します。
- 3 自動プロセスを実行して、ラップトップまたは接続されている USB ドライブにゴールデンテンプレートをエクスポートします。
- 4 カスタマーサイトにゴールデンテンプレート ファイルを転送します。

- 5 自動プロセスを実行して、カスタマー宛先サーバにゴールデンテンプレートをインポートします。
- 6 インポート後の手順を実行します。
- 7 お客様向けに初期設定を実行します。

ゴールデンテンプレートの作成

Cisco Unified Contact Center Enterprise コールサーバ用のゴールデンテンプレートの作成

CCE コールサーバ用のゴールデンテンプレートを作成するには、次の一連のタスクを実行します。このゴールデンテンプレートは、カスタマーサイト（一方が A 側で、もう一方が B 側）で 2 台の仮想マシンとして展開されます。

シーケンス	タスク
1	CCE-PAC-M1_CCE.ova を使用した、 OVA からの仮想マシンの作成 、(85 ページ)。ドロップダウンリストから [CCE コールサーバ (CCE Call Server)] を選択します。
2	Windows Server 2008 のインストール 、(89 ページ)
3	Windows での VM の VMware ツールのインストール 、(91 ページ)
4	コールサーバおよびデータサーバのネットワークアダプタの設定 、(91 ページ)
5	Windows アップデートの実行 、(93 ページ)
6	アンチウイルスソフトウェアのインストール 、(88 ページ)
7	Cisco Unified Contact Center Enterprise のインストール 、(98 ページ)

自動化プロセスの実行後は、宛先システム上で CCE コールサーバを設定できます。[Cisco Unified CCE コールサーバ](#)、(127 ページ) を参照してください。

Cisco Unified Contact Center Enterprise データサーバ用のゴールデンテンプレートの作成

CCE データサーバ用のゴールデンテンプレートを作成するには、次の一連のタスクを実行します。このゴールデンテンプレートは、カスタマーサイト（一方が A 側で、もう一方が B 側）で 2 台の仮想マシンとして展開されます。

シーケンス	タスク
1	CCE-PAC-MI-CCE.ova を使用した、 OVA からの仮想マシンの作成 、(85 ページ)。ドロップダウン リストから [CCE データベース サーバ (CCE Database Server)] を選択します。
2	Windows Server 2008 のインストール 、(89 ページ)
3	Windows での VM の VMware ツールのインストール 、(91 ページ)
4	コール サーバおよびデータ サーバのネットワーク アダプタの設定 、(91 ページ)
5	Windows アップデートの実行 、(93 ページ)
6	アンチウイルス ソフトウェアのインストール 、(88 ページ)
7	Microsoft SQL Server のインストール 、(93 ページ)
8	Cisco Unified Contact Center Enterprise のインストール 、(98 ページ)
9	データベース ドライブの設定 、(87 ページ)

自動化プロセスの実行後は、宛先システム上で CCE データ サーバ VM を設定できます。[Cisco Unified CCE データ サーバ](#)、(115 ページ) を参照してください。

Cisco Unified Customer Voice Portal サーバ用のゴールデン テンプレートの作成

Unified CVP コール/VXML サーバおよび Unified CVP OAMP サーバ用のゴールデン テンプレートを作成するには、次の一連のタスクを実行します。

- Unified CVP コール/VXML サーバがカスタマー サイトで 4 台の仮想マシン (A 側に 2 台および B 側に 2 台) として展開されます。
- Unified CVP OAMP サーバは、A 側の 1 台の仮想マシンとして展開されます。

このプロセスはコール/VXML および OAMP サーバでも同様です。違いは、インストール時に OVA ドロップダウンから、または [パッケージの選択 (Select Packages)] オプションで選択する内容です。

シーケンス	タスク
1	CCE-PAC-MI-CVP.ova を使用した、 OVA からの仮想マシンの作成 、(85 ページ)。ドロップダウン リストで、次の内容を実行します。 <ul style="list-style-type: none"> • コール サーバ VM の作成時に CVP コール サーバを選択する。 • CVP OAMP サーバ VM の作成時に CVP OAMP サーバを選択する。

シーケンス	タスク
2	Windows Server 2008 のインストール , (89 ページ)
3	Windows での VM の VMware ツールのインストール , (91 ページ)
4	Cisco Unified CVP のネットワーク アダプタの設定 , (99 ページ)
5	Windows アップデートの実行 , (93 ページ)
6	アンチウイルス ソフトウェアのインストール , (88 ページ)
7	Cisco Unified CVP サーバのインストール , (98 ページ)

自動化プロセスの実行後は、宛先システム上で Unified CVP VM を設定できます。[Cisco Unified Customer Voice Portal](#), (141 ページ) を参照してください。

Unified CVP Reporting Server 用のゴールデンテンプレートの作成

Unified CVP Reporting Server 用のゴールデンテンプレートを作成するには、次の一連のタスクを実行します。

シーケンス	タスク
1	CCE-PAC-M1-CVP-Reporting.ova を使用した、OVA からの仮想マシンの作成 , (85 ページ)。 ドロップダウンから [CVP Reporting Server] を選択します。
2	Windows Server 2008 のインストール , (89 ページ)
3	Windows での VM の VMware ツールのインストール , (91 ページ)
4	Cisco Unified CVP のネットワーク アダプタの設定 , (99 ページ)
5	Windows アップデートの実行 , (93 ページ)
6	アンチウイルス ソフトウェアのインストール , (88 ページ)
7	Cisco Unified CVP サーバのインストール , (98 ページ)
9	データベース ドライブの設定 , (87 ページ)

自動化プロセスの実行後は、宛先システム上で CVP Reporting Server を設定できます。[Cisco Unified Customer Voice Portal Reporting Server](#), (187 ページ) を参照してください。

Cisco Unified Communications Manager 用のゴールデン テンプレートの作成

A 側の Cisco Unified Communications Manager 用のゴールデン テンプレートを作成するには、次の一連のタスクを実行します。

シーケンス	タスク
1	CCE-PAC-M1-CUCM.ova を使用した、 OVA からの仮想マシンの作成 、(85 ページ)。ドロップダウン リストから 7500 ユーザ ノードを選択します。
2	Cisco Unified Communications Manager パブリッシャのインストール。 VOS ベースのコンタクトセンター アプリケーションに対するゴールデンテンプレートのインストール 、(104 ページ)。

自動化プロセスの実行後は、宛先システムで Unified Communications Manager パブリッシャおよびサブスクリバ VM を設定できます。[Cisco Unified Communications Manager](#)、(157 ページ) を参照してください。

Cisco Finesse 用のゴールデン テンプレートの作成

Cisco Finesse プライマリ ノード用のゴールデン テンプレートを作成するには、次の一連のタスクを実行します。

シーケンス	タスク
1	CCE-PAC-M1-Finesse.ova を使用した、 OVA からの仮想マシンの作成 、(85 ページ)。ドロップダウン リストで選択できる項目はありません。
2	Cisco Finesse プライマリ ノードのインストール。 VOS ベースのコンタクトセンター アプリケーションに対するゴールデンテンプレートのインストール 、(104 ページ)。

自動化プロセスの実行後は、宛先システムで Cisco Finesse を設定できます。[Cisco Finesse](#)、(177 ページ) を参照してください。

Cisco Unified Intelligence Center 用のゴールデン テンプレートの作成

Cisco Unified Intelligence Center パブリッシャ ノード用のゴールデン テンプレートを作成するには、次の一連のタスクを実行します。

シーケンス	タスク
1	CCE-PAC-M1-CUIC.ova を使用した、 OVA からの仮想マシンの作成 、(85 ページ)。ドロップダウン リストで選択できる項目はありません。
2	Cisco Unified Intelligence Center のインストール。 VOS ベースのコンタクトセンターアプリケーションに対するゴールデンテンプレートのインストール 、(104 ページ)。

自動化プロセスの実行後は、宛先システムで Cisco Unified Intelligence Center VM を設定できます。[Cisco Unified Intelligence Center](#)、(171 ページ) を参照してください。



第 5 章

カスタマー サイトでのゴールデン テンプレート の展開

- [ホストの権限, 49 ページ](#)
- [自動ツール, 49 ページ](#)
- [エクスポート用の自動化スプレッドシート の入力, 50 ページ](#)
- [エクスポート用の自動化スクリプト の実行, 51 ページ](#)
- [カスタマー への転送, 52 ページ](#)
- [カスタマー サイトの準備状態の確認, 52 ページ](#)
- [インポート用のスプレッドシート の入力, 53 ページ](#)
- [インポート用の自動化スクリプト の実行, 58 ページ](#)

ホストの権限

ゴールデン テンプレート プロセスを実行しているユーザが ESXi ホストの次の権限を持っている必要があります。

- 管理者
- リソース プール管理者
- ネットワーク管理者

自動ツール

自動化を実行するクライアントに次のツールをダウンロードしてから、インストールします。

ソフトウェア	バージョン	ダウンロード
GoldenTemplateTool zip ファイル	10.5(1)	http://cisco.com/en/US/products/ps12586/tsd_products_support_series_home.html に進みます。 [ソフトウェアのダウンロード (Download Software)] をクリックします。 次に、[Packaged Contact Center Enterprise Deployment Scripts] を選択します。
PowerCLI	5.0 または 5.1、32 ビット	http://downloads.vmware.com/d/details/pcli50/dHRAYnQIKmpiZHAJQ==
OVF ツール	32 ビット	https://my.vmware.com/group/vmware/details?downloadGroup=OVFTOOL350&productId=353
WinImage	8.5、32 ビット	http://winimage.com/download.htm 。 (注) WinImage は、シェアウェアです。ライセンス コピーを購入しない場合、このツールを実行するときにポップアップが表示されます。ポップアップで [いいえ (No)] をクリックすると、次に進めます。
Microsoft Excel	Release 2003 以降	--

エクスポート用の自動化スプレッドシートの入力

エクスポート用の自動化スプレッドシートを入力します。エクスポート自動化スクリプトが GoldenTemplate_10 ディレクトリの OVF サブフォルダにエクスポート OVF の作成を要求する各行のカラムに対してのみ内容を入力します。その他すべてのカラムは空白のままにします。

次の VM_TYPE の行に対してのみ、内容を入力してください。

- UCCE_CallServer_SideA
- UCCE_DataServer_SideA
- CVP_Call/VXML_1_SideA
- CVP_RPT_SideB
- CVP_OAMP_SideA
- CUCM_Pub_SideA
- CUIC_PUB_SideA
- FINESSE_PRIMARY_SideA

インポートフェーズでは、サブスクリバおよび B 側に存在するサーバを含む残りのサーバに対して VM を作成する際に、これらのテンプレートを使用できます。

表 3: エクスポート用の自動化スプレッドシートに必要なカラム

カラム	説明	例
OPERATION	[ExportServer] を選択して、スクリプトで実行している操作を指定します。 テンプレートのシステムがインストールされた VMware 環境から圧縮された OVF ファイルをエクスポートします。	ExportServer
SOURCE_HOST_IP	VM をエクスポートする ESXi ホスティングの IP アドレスまたは DNS 名。	xx.xx.xxx.xxx
SOURCE_DATASTORE_NAME	VMware で定義されたデータストアの名前。	datastore1(3)
SOURCE_VMNAME	VM の名前。スペースや特殊文字は使用できません。最大 32 文字。	CallServerSideA
GOLDEN_TEMPLATE_NAME	エクスポートされるゴールデンテンプレートの名前。スペースや特殊文字は使用できません。最大 32 文字。	My_CallServerA

エクスポート用の自動化スクリプトの実行

エクスポートしたサーバに必要なディスク領域は、エクスポートしたサーバに応じて、50GB ～ 70GB になります。

手順

- ステップ 1** デスクトップの VMWare PowerCLI (32 ビット) アイコンを右クリックし、[Run as Administrator] を選択します。
- ステップ 2** 他のユーザから署名されたスクリプトと同様に、ローカルに書き込む未署名のスクリプトを実行できるように、次のコマンドを入力して、実行ポリシーを変更できます：**Set-ExecutionPolicy Unrestricted -Force**。
- ステップ 3** VMware vSphere PowerCLI が vSphere サーバの接続にプロキシサーバを使用しないように、次のコマンドを入力します：**Set-PowerCLIConfiguration -ProxyPolicy NoProxy -Confirm:\$false**。
- ステップ 4** 次のコマンドを入力します：**cd <Golden Template tool directory>**。
- ステップ 5** 次の構文を使用してコマンドを入力します。

構文：	例：
<スクリプトへのパス><スプレッドシートのフルパス> <vCenter IP / ホスト名> <vCenter ユーザ> <vCenter に接続するためのパスワード>	. \scripts\DeployVM.PS1 c:\GoldenTemplate_VMDataSheet_V10.xls testvCenter testuser testpassword

これは、GoldenTemplate_10 ディレクトリの OVF フォルダのエントリを作成するスクリプトを起動します。スクリプトは通常、数時間以内で完了します。エラーがある場合、スクリプトは失敗しますが、動作し続けます。エラーが画面に表示され、ログファイルに保存されます。スクリプトが完了すると、Report フォルダにステータスレポートが生成されます。ステータスレポートには、ログファイルへのリンクがあります。

カスタマーへの転送

インポート中、動作モードは ImportServer に設定されるので、ゴールデンテンプレートプロセスがカスタマーサイトでエクスポートした OVF テンプレートをインポートします。

ラップトップをカスタマーサイトに接続します。次に、スプレッドシートのインポートを完了し、ローカルディレクトリからインポートスクリプトを実行します。

USB デバイスにディレクトリを転送し、USB ドライブからインポートスクリプトを実行することもできます。

カスタマーサイトの準備状態の確認

インポートスプレッドシートを記入し、インポートスクリプトを実行する前に、データストアが設定され、ホストが vCenter に登録されている ESXi ホストで、顧客の環境を設定する必要があります。

インポート用のスプレッドシートの入力

インポート用にスプレッドシートのすべての行を入力します。複数の VM をインポートするために同じテンプレートを使用できます。NEW_VM_NAME などの他のカラムは一意である必要がありますが、GOLDEN_TEMPATE_NAME は、たとえば GOLDEN_TEMPATE_NAME は、UCCE_DataServer_SideA および UCCE_DataServer_SideB の両方で同じにすることができます。

表 4: インポート用の自動化スプレッドシートカラムの入力

カラム	説明	例
CREATEVM	[はい (YES)] を選択して、VM を作成します。	はい (YES)
CUSTOMIZATION	[はい (YES)] を選択して、インポートされたサーバにスプレッドシートの値を適用します。 (注) [はい (Yes)] を選択すると、VOS 製品のパブリッシャとサブスクライバが作成されます。	はい (YES)
OPERATION	[ImportServer] を選択します。 エンドカスタマーの VMware 環境に OVF テンプレートをインポートします。	ImportServer
SOURCE_HOST_IP	ブランクのままにします。	ブランクのままにします。
SOURCE_DATASTORE_NAME	ブランクのままにします。	ブランクのままにします。
SOURCE_VMNAME	ブランクのままにします。	ブランクのままにします。
GOLDEN_TEMPLATE_NAME	エクスポートされたゴールデンテンプレートの名前を入力します。	My_CallServerA
NEW_VM_NAME	必須作業です。新しい VM の名前。スペースや特殊文字は使用できません。最大 32 文字。	CallServerSideA

カラム	説明	例
DEST_HOST_IP	必須作業です。新しい VM の ESXi ホストの IP アドレスまたは DNS 名。	xx.xx.xxx.xxx
DEST_DATASTORE_NAME	必須作業です。新しい VM のデータストアの名前。	datastore2(1)
PRODUCT_VERSION	このフィールドは、すべての VOS プラットフォームに適用されます。	
COMPUTER_NAME	必須作業です。新しいコンピュータの NET BIOS 名。最大 15 文字。特殊文字 \、?、:、*、"、<、>、. は使用しないでください。	Demo-CallSrvA
WORK_GROUP	ドロップダウン : [はい (YES)] は、VM をワークグループに追加し、WORK_GROUP_NAME を有効にします。	NO
WORK_GROUP_NAME	WORK_GROUP が [はい (YES)] に設定されている場合にだけワークグループの名前を入力します。	NA
DOMAIN_NAME	ドメインの名前。 WORK_GROUP が [いいえ (NO)] に設定された場合にのみ使用されます。	mydomain.com
TIME_ZONE_LINUX_AREA	必須作業です。Unified CM に設定されるタイムゾーン地域のドロップダウン選択。米国の場合は、[アメリカ (America)] を選択します。	アメリカ (America)
TIME_ZONE_LINUX_LOCATION	必須作業です。Unified CM、CUIC、または Finesse に設定されるタイムゾーンの場所のドロップダウン選択。	New York

カラム	説明	例
TIME_ZONE_WINDOWS	必須作業です。 Unified CVP および Unified CCE VM に設定されるタイムゾーンのドロップダウン選択。	(GMT-05:00) 東部時間帯 (米国およびカナダ)
DOMAIN_USER	必須作業です。 新しいコンピュータをドメインに追加する権限を持つドメイン ユーザのユーザ名。 WORK_GROUP が [いいえ (NO)] に設定されている場合にだけ有効です。 <i>DOMAIN\username</i> または <i>username@</i> 形式でユーザ名を指定しないでください。	ユーザ名 (Username)
DOMAIN_PASSWORD	必須作業です。 ドメイン ユーザのパスワード。 WORK_GROUP が [いいえ (NO)] に設定されている場合にだけ有効です。	package123
PRODUCT_KEY	必須作業です。 形式 XXXXX-XXXXX-XXXXX-XXXXX-XXXXX の有効な Windows OS のプロダクトキー。	ZZM2-Y330L-HH123-99Y1B-GJ20B
OWNER_NAME	必須作業です。 所有者の完全な名前。 <i>Administrator</i> および <i>Guest</i> は使用できない名前です。 これは Windows の必須フィールドです。	LabAdmin
ORGANIZATION_NAME	必須作業です。 Unified CM、CUIC、または Finesse に設定する組織名。	MyName
ORGANIZATION_UNIT	必須作業です。 Unified CM、CUIC、または Finesse に設定する組織ユニット。	MyUnit

カラム	説明	例
ORGANIZATION_LOCATION	必須作業です。 Unified CM、CUIC、または Finesse に設定する組織の場所。	MyCity
ORGANIZATION_STATE	必須作業です。 Unified CM、CUIC、または Finesse に設定する組織の都道府県。	MyState
ORGANIZATION_COUNTRY	必須作業です。 Unified CM、CUIC、または Finesse に設定する組織の国のドロップダウン選択。	米国 (United States of America)
NTP_SERVER NTP および時刻同期, (21 ページ) を参照してください。	必須作業です。 NTP サーバの IP アドレス。	xx.xx.xxx.xxx
IP_ADDRESS_NIC1	必須作業です。 NIC1 の有効な IPv4 アドレス。	xx.xx.xxx.xxx
SUB_NET_MASK_NIC1	必須作業です。 NIC1 の有効なサブネットマスク (IPv4 アドレス)。	xx.xx.xxx.xxx
NIC_NUM	フィールドの値は、VM_TYPE フィールドに基づいて事前に入力され、保護されます。値は「1」または「2」です。 この値は、VM に設定される NIC の数を示しています。	2
DEFAULT_GATEWAY_NIC1	必須作業です。 NIC1 の有効なデフォルトゲートウェイ (IPv4 アドレス)。	xx.xx.xxx.xxx
DNS_IP_NIC1	必須作業です。 NIC1 のプライマリ DNS の有効な IPv4 アドレス。	xx.xx.xxx.xxx

カラム	説明	例
DNS_ALTERNATE_NIC2	これはオプションです。NIC1の代替DNSの有効なIPv4アドレス。Unified CCE VM専用。NIC1のプライマリDNSのアドレスとは異なる必要があります。	xx.xx.xxx.xxx
IP_ADDRESS_NIC2	必須作業です。NIC2の有効なIPv4アドレス。 NIC_NUM フィールドの値が2の場合にのみ有効です。	xx.xx.xxx.xxx
SUB_NET_MASK_NIC2	必須作業です。NIC2の有効なサブネットマスク (IPv4アドレス)。Unified CCE VM専用。	255.255.255.255
DEFAULT_GATEWAY_NIC2	必須作業です。NIC2の有効なデフォルトゲートウェイ (IPv4アドレス)。 これは後で削除されますが、カスタマイズ中に必要です。	xx.xx.xxx.xxx
DNS_IP_NIC2	必須作業です。NIC2のプライマリDNSの有効なIPv4アドレス。Unified CCE VM専用。 これは後で削除されますが、カスタマイズ中に必要です。	xx.xx.xxx.xxx
DNS_ALTERNATE_NIC2	これはオプションです。NIC2の代替DNSの有効なIPv4アドレス。Unified CCE VM専用。NIC2のプライマリDNSのアドレスとは異なる必要があります。	xx.xx.xxx.xxx
VM_NETWORK	必須作業です。このサーバのプライマリネットワーク	UCCE Public

インポート用の自動化スクリプトの実行

スクリプトはテンプレートをインポートし、新規の VM を作成します。



(注) 任意の VOS VM をインポートし、WinImage のアンライセンスドコピーがある場合は、各 VOS のプラットフォームに 1 つのポップアップ ダイアログが表示されます。[OK] をクリックして、インポート プロセスを続行します。

手順

- ステップ 1 デスクトップの VMWare PowerCLI (32 ビット) アイコンを右クリックし、[Run as Administrator] を選択します。
- ステップ 2 他のユーザから署名されたスクリプトと同様に、ローカルに書き込む未署名のスクリプトを実行できるように、次のコマンドを入力して、実行ポリシーを変更できます：**Set-ExecutionPolicy Unrestricted -Force**。
- ステップ 3 VMware vSphere PowerCLI が vSphere サーバの接続にプロキシサーバを使用しないように、次のコマンドを入力します：**Set-PowerCLIConfiguration -ProxyPolicy NoProxy -Confirm:\$false**。
- ステップ 4 次のコマンドを入力します：**cd <Golden Template tool directory>**。
- ステップ 5 次の構文を使用してコマンドを入力します。

構文：	例：
<スクリプトへのパス><スプレッドシートのフルパス> <vCenter IP / ホスト名> <vCenter ユーザ> <vCenter に接続するためのパスワード>	. \scripts\DeployVM.PS1 c:\GoldenTemplate_VMDataSheet_V10.xls testvCenter testuser testpassword

スクリプトは通常、数時間以内で完了します。エラーがある場合、スクリプトは失敗しますが、動作し続けます。エラーが画面に表示され、ログファイルに保存されます。スクリプトが完了すると、Report フォルダにステータス レポートが生成されます。ステータス レポートには、ログファイルへのリンクがあります。

Status Report of Golden Template to VM conversion

VM NAME	DESTINATION HOST	DESTINATION DATASTORE	STATUS	DESCRIPTION
CallServerSideA	203.0.113.84	EMC2-disk15 600GB FC 10DSK R5 RG13 LUN13	Success	VM deployed successfully
DataServerSideA	203.0.113.84	EMC2-disk15 600GB FC 10DSK R5 RG13 LUN13	Success	VM deployed successfully
CallServerSideB	203.0.113.85	EMC2-disk15 600GB FC 10DSK R5 RG13 LUN13	Success	VM deployed successfully
DataServerSideB	203.0.113.85	EMC2-disk15 600GB FC 10DSK R5 RG13 LUN13	Success	VM deployed successfully
CVPCallServerSide1A	203.0.113.84	EMC2-disk20 600GB FC 10DSK R5 RG15 LUN18	Success	VM deployed successfully
CVPCallServerSide2A	203.0.113.84	EMC2-disk20 600GB FC 10DSK R5 RG15 LUN18	Success	VM deployed successfully
CVPCallServerSide1B	203.0.113.85	EMC2-disk20 600GB FC 10DSK R5 RG15 LUN18	Success	VM deployed successfully
CVPCallServerSide2B	203.0.113.85	EMC2-disk20 600GB FC 10DSK R5 RG15 LUN18	Success	VM deployed successfully
CVPRPTSIDEA	203.0.113.84	EMC2-disk20 600GB FC 10DSK R5 RG15 LUN18	Success	VM deployed successfully
CVPOAMPSIDEB	203.0.113.84	EMC2-disk20 600GB FC 10DSK R5 RG15 LUN18	Success	VM deployed successfully
CUCM_PUB_SideA	203.0.113.84	EMC2-disk20 600GB FC 10DSK R5 RG15 LUN18	Success	VM deployed successfully
CUCM_SUB_SideA	203.0.113.84	EMC2-disk20 600GB FC 10DSK R5 RG15 LUN18	Success	VM deployed successfully
CUCM_SUB_SideB	203.0.113.85	EMC2-disk20 600GB FC 10DSK R5 RG15 LUN18	Success	VM deployed successfully
CUIC_PUB_SideA	203.0.113.84	EMC2-disk20 600GB FC 10DSK R5 RG15 LUN18	Success	VM deployed successfully
CUIC_SUB_SideA	203.0.113.84	EMC2-disk20 600GB FC 10DSK R5 RG15 LUN18	Success	VM deployed successfully
Fmesse_PUB	203.0.113.84	EMC2-disk24 600GB FC 5DSK R5 RG16 LUN22	Success	VM deployed successfully
Fmesse_SUB	203.0.113.85	EMC2-disk24 600GB FC 5DSK R5 RG16 LUN22	Success	VM deployed successfully

28/416



第 6 章

ゴールデン テンプレートのインポート後

- [データ サーバのインポート後の手順, 61 ページ](#)
- [コール サーバのインポート後の手順, 62 ページ](#)
- [Cisco Unified Voice Portal のインポート後の手順, 62 ページ](#)
- [Cisco Unified Communications Manager のインポート後の手順, 62 ページ](#)
- [Cisco Unified Intelligence Center のインポート後の手順, 63 ページ](#)
- [Cisco Finesse のインポート後の手順, 63 ページ](#)
- [インポート後の手順, 63 ページ](#)

データ サーバのインポート後の手順

コール サーバのインポート後に、次の手順を実行します。

シーケンス	タスク
1	ネットワーク アダプタ設定と電源投入の検証, (63 ページ)
2	レジストリ設定の編集と VM の再起動, (66 ページ)
3	ネットワーク アダプタの名前の変更と再バインド, (66 ページ)
4	Unified CCE 暗号化ユーティリティの設定, (64 ページ)
5	Cisco Diagnostic Framework Portico の設定, (64 ページ)
6	セキュリティ ウィザードの実行, (68 ページ)
7	ドメイン ユーザの追加, (65 ページ)
8	Cisco Unified CCE データ サーバ, (115 ページ) の設定

コール サーバのインポート後の手順

コール サーバのインポート後に、次の手順を実行します。

シーケンス	タスク
1	ネットワーク アダプタ設定と電源投入の検証, (63 ページ)
2	レジストリ設定の編集と VM の再起動, (66 ページ)
3	ネットワーク アダプタの名前の変更と再バインド, (66 ページ)
4	Unified CCE 暗号化ユーティリティの設定, (64 ページ)
5	Cisco Diagnostic Framework Portico の設定, (64 ページ)
6	セキュリティ ウィザードの実行, (68 ページ)
7	Cisco Unified CCE コール サーバ, (127 ページ) の設定

Cisco Unified Voice Portal のインポート後の手順

Unified CVP サーバのインポート後に、次の手順を実行します。

シーケンス	タスク
1	ネットワーク アダプタ設定と電源投入の検証, (63 ページ)
2	レジストリ設定の編集と VM の再起動, (66 ページ)
4	時刻源のリセット, (68 ページ)
5	Cisco Unified Customer Voice Portal, (141 ページ) の設定

Cisco Unified Communications Manager のインポート後の手順

Cisco Unified Communications Manager のインポート後に、次の手順を実行します。

タスク	シーケンス
1	Unified Communications Manager パブリッシャの設定, (69 ページ)
2	サブスクリイバを追加するための Unified Communications Manager パブリッシャの起動, (69 ページ)

タスク	シーケンス
3	Unified Communications Manager サブスクリバの設定 , (70 ページ)
4	Cisco Unified Communications Manager , (157 ページ) の設定

Cisco Unified Intelligence Center のインポート後の手順

Cisco Unified Intelligence Center のインポート後に、次の手順を実行します。

タスク	シーケンス
1	Unified Intelligence Center パブリッシャの設定 , (70 ページ)
2	オンラインでのライセンスの取得, (71 ページ)
3	サブスクリバを追加するためのパブリッシャの起動, (72 ページ)
4	サブスクリバの設定, (72 ページ)
5	Cisco Unified Intelligence Center , (171 ページ) の設定

Cisco Finesse のインポート後の手順

Cisco Finesse のインポート後に、次の手順を実行します。

タスク	シーケンス
1	Cisco Finesse プライマリ ノードの設定 , (73 ページ)
2	セカンダリ Finesse を設定するための Finesse 管理コンソールの起動, (74 ページ)
3	セカンダリ ノードの設定, (73 ページ)
4	Cisco Finesse , (177 ページ) の設定

インポート後の手順

ネットワーク アダプタ 設定と電源投入の検証

すべての Windows VM について、この手順を実行します。

手順

-
- ステップ 1 vSphere クライアントで [仮想マシン (Virtual Machine)] を選択します。 VM を右クリックして、 [設定の編集 (Edit settings)] を選択します。
 - ステップ 2 [ハードウェア (Hardware)] タブで、各ネットワークアダプタを選択します。 デバイスステータスグループで [電源オンで接続 (Connect at power on)] がオンになっていることを確認します。
 - ステップ 3 仮想マシンの電源をオンにします。
重要 Ctrl-Alt-Delete を押さないでください。 電源投入後に Ctrl+Alt+Delete を押した場合、カスタマイズは反映されません。 手動でカスタマイズを完了する必要があります。 詳細については、 http://docwiki.cisco.com/wiki/Recover_from_Pressing_Ctrl-Alt-Del_During_Power-On を参照してください。
 - ステップ 4 VM が再起動し、カスタマイズが適用されるまで待ちます。 この処理に 5 ～ 10 分かかることがあります。
-

Cisco Diagnostic Framework Portico の設定

手順

-
- ステップ 1 [スタート (Start)] メニューで、 [コマンドプロンプト (Command Prompt)] を右クリックして [管理者として実行 (Run as Administrator)] を選択します。
 - ステップ 2 `cd icm\serviceability\diagnostics\bin` と入力し、 Enter を押します。
 - ステップ 3 `DiagFwCertMgr /task:CreateAndBindCert /port:7890` と入力し、 Enter を押します。
-

Unified CCE 暗号化ユーティリティの設定

手順

-
- ステップ 1 [すべてのプログラム (All Programs)] > [Cisco Unified CCE ツール (Cisco Unified CCE Tools)] を起動します。
 - ステップ 2 [SSL 暗号化ユーティリティ (SSL Encryption Utility)] を選択します。
 - ステップ 3 [証明書の管理 (Certificate Administration)] タブをクリックします。
 - ステップ 4 [アンインストール (Uninstall)] をクリックします。 [はい (Yes)] を選択します。
 - ステップ 5 アンインストールが完了したら、 [インストール (Install)] を選択します。

メッセージが次々と表示され、最後に「SSL証明書が正常にインストールされました (SSL Certificate successfully installed)」と表示されます。

ステップ 6 [閉じる (Close)] をクリックします。

ドメインユーザの追加

データ サーバをインポートした後、明示的なログインアカウントとして Web セットアップを実行するドメイン ユーザを SQL Server Manager に追加する必要があります。この手順を A 側と B 側のデータ サーバで実行します。

手順

- ステップ 1** ローカルまたはドメイン管理者としてデータ サーバにログインします。
- ステップ 2** [スタート (Start)] > [すべてのプログラム (All Programs)] > [Microsoft SQL Server 2008 R2] に移動します。
- ステップ 3** [SQL Server Management Studio] を右クリックして [管理者として実行 (Run as administrator)] を選択します。
- ステップ 4** [ユーザアカウント制御 (User Account Control)] ダイアログボックスで [はい (Yes)] を選択します。
- ステップ 5** Windows 認証を使用して SQL Server に接続します。
- ステップ 6** [Object Explorer] で、[セキュリティ (Security)] ツリーを展開します。
- ステップ 7** [ログイン (Logins)] を右クリックし、[新しいログイン... (New Login...)] を選択します。
- ステップ 8** [新規ログイン (New Login)] ダイアログボックスで、次の内容を実行します。
- a) Windows 認証が選択されているのを確認して、[検索 (Search)] をクリックします。
 - b) [ユーザまたはグループの選択 (Select User or Group)] ダイアログボックスで、次の手順を実行します。
 - 1 場所を [ディレクトリ全体 (Entire Directory)] に設定します。
 - 2 ドメインユーザのアカウント名を入力します。
 - 3 [名前のチェック (Check Names)] を選択し、ボックスに正しい名前が表示されることを確認します。
 - 4 [OK] をクリックします。
 - c) [新規ログイン (New Login)] ダイアログボックスの [サーバロール (Server Roles)] ページに移動し、[public] と [sysadmin] の両方がオンになっていることを確認します。

d) [OK] をクリックして変更を保存します。

ステップ 9 SQL Server Management Studio を終了します。

ステップ 10 ログアウトし、ドメイン ユーザとして再度ログインします。

ステップ 11 通常どおりに SQL Server Management Studio ([管理者として実行 (Run as administrator)] を使用しない) を実行して、Windows 認証を使用してログインし、変更内容を確認します。

レジストリ設定の編集と VM の再起動

すべての Windows VM について、この手順を実行します。

手順

ステップ 1 [スタート (Start)] > [管理ツール (Administrative Tools)] > [コンピュータの管理 (Computer Management)] に移動します。

ステップ 2 左側のパネルで、[コンピュータ管理 (ローカル) (Computer Management (Local))] > [システムツール (System Tools)] > [ローカル ユーザおよびグループ (Local Users and Groups)] > [ユーザ (Users)] を選択します。

ステップ 3 右側のパネルで、[管理者 (Administrator)] を右クリックし、[パスワードの設定 (Set Password)] を選択します。

ステップ 4 警告メッセージで [続行 (Proceed)] をクリックし、新しいパスワードを入力します。

ステップ 5 [OK] をクリックして保存します。

ステップ 6 レジストリエディタにアクセスします ([スタート (Start)] > [ファイル名を指定して実行 (Run)] > **regedit**)。

ステップ 7 [HKEY_LOCAL_MACHINE] > [SOFTWARE] > [Microsoft] > [Windows NT] > [Current Version] > [Winlogon] に移動します。

a) [AutoAdminLogon] を **0** に設定します。

b) 存在する場合は次のキーを削除します: [DefaultDomainName] および [DefaultUserName]。

ステップ 8 マシンを再起動します。マシンがドメインに存在する場合は、ドメインにログインします。

ステップ 9 時刻をドメインコントローラと同期するには、コマンドプロンプトを開き、コマンド **NET TIME /DOMAIN:<domain>** と入力します。

ネットワーク アダプタの名前の変更と再バインド

コール サーバとデータ サーバのゴールデン テンプレートをインポートした後、ネットワーク アダプタを再設定する必要があります。

手順

- ステップ 1** 次の手順に従って、ネットワーク アダプタの MAC アドレスとラベルを特定します。
- vCenter から、VM を選択し、右クリックします。
 - [設定の編集 (Edit Settings)] を選択します。[ハードウェア (Hardware)] タブで、[ネットワーク アダプタ 1 (Network adapter 1)] をクリックします。右側のパネルで、MAC アドレスの最後の数桁を書き留め、ラベルが UCCE パブリックまたは UCCE プライベートかどうかをメモします。たとえば、ネットワーク アダプタ 1 の MAC アドレスは 08-3b で終わり、ネットワーク ラベルが UCCE パブリックである可能性があります。
 - ネットワーク アダプタ 2 で繰り返します。MAC アドレスとラベルをメモします。
 - VM コンソールで、コマンドラインから `ipconfig /all` と入力します。これはアダプタ名と物理アドレスを表示します。
 - アダプタ名と物理アドレスをメモし、VMware でメモした MAC アドレスとラベルと照合します。たとえば、`ipconf/all` では、ローカルエリア接続 2 の物理アドレスは、08-3b で終了する可能性があります。
 - VMware が UCCE パブリックとして識別したネットワーク アダプタの MAC アドレスを、ローカルエリアコネクタの対応する物理アドレスと照合します。この例では、ローカルエリア接続 2 (08-3b) の物理アドレスがネットワーク アダプタ 1 の MAC アドレス (08-3b) に一致します。ローカルエリア接続 2 が UCCE パブリックであることを意味します。
- ステップ 2** 次のように、Windows のネットワーク アダプタを検索して、名前を変更します。
- [ネットワークと共有センター (Network and Sharing Center)] を開き、[ローカル エリア接続 (Local Area Connection)] を選択します。
 - [ローカル エリア接続 (Local Area Connection)] を右クリックして、[名前の変更 (Rename)] を選択します。上記の照合に応じて、[UCCE Public] または [UCCE Private] に名前を変更します。
 - [ローカル エリア接続 2 (Local Area Connection 2)] を右クリックして、[名前の変更 (Rename)] を選択します。上記の照合に応じて、[UCCE Public] または [UCCE Private] に名前を変更します。上記の例では、[ローカル エリア接続 2 (Local Area Connection 2)] が UCCE パブリックに名前が変更されます。
- ステップ 3** 次のように UCCE プライベートのプロパティを設定します。
- `c:\windows\system32\drivers\etc` に移動し、ホストファイルを編集して、サーバの IP アドレスおよび完全修飾ドメイン名を使用してエントリを追加します。
 - DNS サーバでは、プライベート IP アドレスのエントリを追加します。この IP のホスト名に *p* などのサフィックスを追加します (プライベートであることを識別するため)。
- ステップ 4** バインディング順序は、次のように設定します。
- [ネットワーク接続 (Network Connections)] では、Alt キーを押します。次に、[詳細 (Advanced)] > [詳細設定 (Advanced Settings)] を選択します。

- b) [アダプタおよびバインディング (Adapters and Bindings)] ダイアログボックスの上部パネルでは、UCCE パブリック接続が UCCE プライベート接続の上にあることを確認します。正しい順序に並べ替える必要がある場合、矢印ボタンを使用します。[OK] をクリックします。

セキュリティ ウィザードの実行

インポート後、すべてのコール サーバおよびデータ サーバでこの手順を実行します。

手順

- ステップ 1** [スタート (Start)] > [すべてのプログラム (All Programs)] > [Cisco Unified CCE ツール (Cisco Unified CCE Tools)] > [Security Wizard] に移動します。
- ステップ 2** [Windows ファイアウォール (Windows Firewall)] をクリックして [次へ (Next)] をクリックします。
- ステップ 3** [ICM/CCE に Windows ファイアウォールを設定 (Configure Windows Firewall for ICM/CCE)] を選択します。[次へ (Next)] をクリックします。
- ステップ 4** [終了 (Finish)] をクリックします。プロンプトで [はい (Yes)] をクリックします。

時刻源のリセット

すべての CVP サーバについて、この手順を実行します。

- 1 [コマンドプロンプト (Command Prompt)] ウィンドウで、次の行を入力して、Enter キーを押します。`w32tm /config /manualpeerlist:PEERS /syncfromflags:MANUAL`



(注) NTP サーバのカンマ区切りリストを使用して、ピアを置き換えます。

- 2 `w32time` サービスを再開します：`net stop w32time && net start w32time`。
- 3 ピアと `w32time` サービスを同期します：`w32tm /resync`。
- 4 次のサービス コントロール コマンドを使用して、サーバの再起動で `w32time` サービスが適切に起動していることを確認します：`sc triggerinfo w32time start/networkon stop/networkoff`。

Unified Communications Manager パブリッシャの設定

はじめる前に

Unified Communications Manager、Cisco Unified Intelligence Center、および Cisco Finesse 用の DNS 設定が必須です。DNS を設定するには、VM を DNS の前方および逆引き参照に追加します。詳細については、[DNS サーバの設定](#)、(87 ページ) を参照してください。

手順

-
- ステップ 1** パブリッシャの電源を投入します。
インストールは自動的に開始され、実行中に行う操作はありません。1 時間以上経過した後、インストールの成功を示すメッセージが表示されます。
 - ステップ 2** VM の [コンソール (Console)] タブをクリックします。管理者ユーザのクレデンシャルを使用して、パブリッシャ マシンにログインします。
 - ステップ 3** 設定を編集し、フロッピー ドライブの [電源投入時に接続 (Connect at Power on)] をオフにします。
-



- (注) パブリッシャ/プライマリのカスタマイズ中、ユーザ名とパスワードが次のように変更されます。お客様はパスワードを変更する必要があります。[カスタマイズ中のパスワード変更](#)、(74 ページ) を参照してください。
-

リブート後に、VM のインストールが完了します。

サブスクライバを追加するための Unified Communications Manager パブリッシャの起動

サブスクライバを追加するには、パブリッシャ ノードを起動する必要があります。

手順

-
- ステップ 1 ブラウザで Unified Communications Manager パブリッシャ (<http://<IP Addr of CUCM Publisher>/ccmadmin>) を起動します。
 - ステップ 2 ユーザ名とパスワードを入力し、Unified Communications Manager にログインします。
 - ステップ 3 [システム (System)] > [サーバ (Server)] > [新規追加 (Add New)] を選択します。
 - ステップ 4 [サーバを追加 (Add a Server)] ページで、サーバタイプの [CUCM Voice/Video] を選択します。
[次へ (Next)] をクリックします。
 - ステップ 5 [サーバ情報 (Server Information)] ページで、最初のサブスクライバの IP アドレスを入力します。
 - ステップ 6 [保存 (Save)] をクリックします。
 - ステップ 7 2 番目のサブスクライバについてステップ 3 ~ 6 を繰り返します。
-

Unified Communications Manager サブスクライバの設定

はじめる前に

Unified Communications Manager、Cisco Unified Intelligence Center、および Cisco Finesse 用の DNS 設定が必須です。DNS を設定するには、VM を DNS の前方および逆引き参照に追加します。詳細については、[DNS サーバの設定](#)、(87 ページ) を参照してください。

手順

-
- ステップ 1 VM の電源をオンにします。
これは、インストールを開始します。
 - ステップ 2 インストールが完了したら、フロッピー ドライブの [電源投入時に接続 (Connect at Power on)] をオフにします。
 - ステップ 3 B 側の 2 番目のサブスクライバに対してこの手順を繰り返します。
-

Unified Intelligence Center パブリッシャの設定

はじめる前に

Unified Communications Manager、Cisco Unified Intelligence Center、および Cisco Finesse 用の DNS 設定が必須です。DNS を設定するには、VM を DNS の前方および逆引き参照に追加します。詳細については、[DNS サーバの設定](#)、(87 ページ) を参照してください。

手順

- ステップ 1** パブリッシャの電源を投入します。
インストールは自動的に開始され、実行中に行う操作はありません。1 時間以上経過した後、インストールの成功を示すメッセージが表示されます。
- ステップ 2** VMの[コンソール (Console)] タブをクリックします。管理者ユーザのクレデンシャルを使用して、パブリッシャマシンにログインします。マシンのCLI インターフェイスが開きます。
- ステップ 3** 設定を編集し、フロッピードライブの[電源投入時に接続 (Connect at Power on)] をオフにします。



- (注) パブリッシャ/プライマリのカスタマイズ中、ユーザ名とパスワードが次のように変更されます。お客様はパスワードを変更する必要があります。[カスタマイズ中のパスワード変更](#)、([74 ページ](#)) を参照してください。

オンラインでのライセンスの取得

パブリッシャを設定した後、サブスクライバを設定する前に、シスコに連絡して Unified Intelligence Center ライセンスを要求する必要があります。

手順

- ステップ 1** ライセンス ファイルを取得するには、次の URL のシスコの製品ライセンス登録 Web サイトに移動します：<https://tools.cisco.com/SWIFT/LicensingUI/Home>。
- ステップ 2** 製品認証キー (PAK) を持っていない場合は、[使用可能なライセンスのリンク](#) をクリックします。
- ステップ 3** [Unified communications] までスクロールし、[Cisco Unified Intelligence Center] をクリックします。
- ステップ 4** MAC アドレスを入力し、契約内容に同意して、登録者情報を入力します。
MAC アドレスは、インストールの最後にオンラインで表示されます。MAC アドレスを再度検出する必要がある場合は、取得するために次の手順に従ってください。
- 1 システム管理者ユーザのクレデンシャルを使用して、サーバノードにサインインします。
 - 2 次の CLI コマンドを入力します。show status
- ステップ 5** プロンプトに従って登録を完了します。
シスコから、ライセンス ファイルが添付ファイルとして含まれている電子メールを受け取ります。ファイル形式は *.lic です。
- ステップ 6** システムアプリケーションユーザがアクセスできる場所にライセンス ファイルを保存します。
警告 このファイルのバックアップ コピーを保存します。*.lic ファイルは、開いて参照できませんが、。このファイルを変更すると、ライセンスが無効になります。

ステップ 7 ライセンスを適用します。

サブスクリイバを追加するためのパブリッシャの起動

手順

- ステップ 1** ブラウザで URL `http://<HOST ADDRESS>/oamp` にアクセスします。ここで、HOST ADDRESS は Cisco Unified Intelligence Center パブリッシャの IP アドレスまたはホスト名です。
 - ステップ 2** インストール時に定義したシステム アプリケーション ユーザ ID とパスワードを使用してサインインします。
 - ステップ 3** 左のパネルから、[デバイス管理 (Device Management)] > [デバイス設定 (Device Configuration)] を選択します。
 - ステップ 4** [メンバーの追加 (Add Member)] をクリックします。
 - ステップ 5** サブスクリイバ用の [デバイス設定 (Device Configuration)] の各フィールドに、デバイスの名前、ホスト名または IP アドレス、および説明を入力します。
 - ステップ 6** [保存 (Save)] をクリックします。
-

サブスクリイバの設定

はじめる前に

Unified Communications Manager、Cisco Unified Intelligence Center、および Cisco Finesse 用の DNS 設定が必須です。DNS を設定するには、VM を DNS の前方および逆引き参照に追加します。詳細については、[DNS サーバの設定](#)、(87 ページ) を参照してください。

手順

- ステップ 1** VM の電源を投入します。
これは、インストールを開始します。
 - ステップ 2** インストールが完了したら、フロッピー ドライブの [電源投入時に接続 (Connect at Power on)] をオフにします。
(注) サブスクリイバノードのカスタマイズ中、ユーザ名とパスワードが次のように変更されます。お客様はパスワードを変更する必要があります。[カスタマイズ中のパスワード変更](#)、(74 ページ) を参照してください。
-

Cisco Finesse プライマリ ノードの設定

はじめる前に

Unified Communications Manager、Cisco Unified Intelligence Center、および Cisco Finesse 用の DNS 設定が必須です。DNS を設定するには、VM を DNS の前方および逆引き参照に追加します。詳細については、[DNS サーバの設定](#)、(87 ページ) を参照してください。

手順

-
- ステップ 1** パブリッシャの電源を投入します。
インストールは自動的に開始され、実行中に行う操作はありません。1 時間以上経過した後、インストールの成功を示すメッセージが表示されます。
- ステップ 2** VM の [コンソール (Console)] タブをクリックします。管理者ユーザのクレデンシャルを使用して、パブリッシャ マシンにログインします。マシンの CLI インターフェイスが開きます。
- ステップ 3** 設定を編集し、フロッピー ドライブの [電源投入時に接続 (Connect at Power on)] をオフにします。
-



- (注) パブリッシャ/プライマリのカスタマイズ中、ユーザ名とパスワードが次のように変更されます。お客様はパスワードを変更する必要があります。[カスタマイズ中のパスワード変更](#)、(74 ページ) を参照してください。
-

セカンダリ ノードの設定

はじめる前に

Unified Communications Manager、Cisco Unified Intelligence Center、および Cisco Finesse 用の DNS 設定が必須です。DNS を設定するには、VM を DNS の前方および逆引き参照に追加します。詳細については、[DNS サーバの設定](#)、(87 ページ) を参照してください。

手順

-
- ステップ 1** VM の電源を投入します。
これは、インストールを開始します。
- ステップ 2** 設定を編集し、フロッピー ドライブの [電源投入時に接続 (Connect at Power on)] をオフにします。

- (注) サブスクライバ ノードのカスタマイズ中、ユーザ名とパスワードが次のように変更されます。お客様はパスワードを変更する必要があります。[カスタマイズ中のパスワード変更](#)、(74 ページ) を参照してください。

- ステップ 3** インストールが完了したら、フロッピー ドライブの [電源投入時に接続 (Connect at Power on)] をオフにします。

セカンダリ Finesse を設定するための Finesse 管理コンソールの起動

セカンダリ ノードを追加するには、プライマリ ノードを起動し、セカンダリ ノードをクラスタに追加する必要があります。

手順

- ステップ 1** ブラウザで Cisco Finesse プライマリ ノードを起動します (<http://Primary Node IP Address/cfadmin>)。ここで、Primary Node または IP Address は自分のホストのプライマリ ノードまたは IP アドレスです。
- ステップ 2** [設定 (Settings)] > [クラスタ設定 (Cluster Settings)] に移動します。(これは、デフォルト設定に基づいており、クラスタ設定ツールのページを変更していないことが前提となります)。
- ステップ 3** Cisco Finesse セカンダリ ノードの IP アドレスを追加します。
- ステップ 4** [保存 (Save)] をクリックします。

カスタマイズ中のパスワード変更



(注) パブリッシュ/プライマリのカスタマイズ中、ユーザ名とパスワードが次のように変更されます。お客様はパスワードを変更する必要があります。

- OS 管理者のデフォルト パスワード : cisco@123
- アプリケーション ユーザ名 : Administrator
- アプリケーション ユーザのデフォルト パスワード : cisco@123
- SFTP パスワード : cisco@123
- IPSec パスワード : cisco@123



第 7 章

直接インストール

- [直接インストールについて](#), 75 ページ
- [Cisco Unified Contact Center Enterprise コール サーバ用の VM の作成](#), 76 ページ
- [Cisco Unified Contact Center Enterprise データ サーバ用の VM の作成](#), 76 ページ
- [Cisco Unified Customer Voice Portal サーバ用の VM の作成](#), 77 ページ
- [Cisco Unified Communications Manager パブリッシャ用の VM の作成](#), 78 ページ
- [Cisco Unified Communications Manager サブスクリバ用の VM の作成](#), 78 ページ
- [Cisco Finesse プライマリ用の VM の作成](#), 79 ページ
- [Cisco Finesse セカンダリ用の VM の作成](#), 79 ページ
- [Cisco Unified Intelligence Center パブリッシャ用の VM の作成](#), 80 ページ
- [Cisco Unified Intelligence Center サブスクリバの VM の作成](#), 80 ページ
- [Cisco Unified CVP Reporting Server 用の VM の作成](#), 80 ページ

直接インストールについて

ここでは、カスタマー宛先サーバに仮想マシンを直接作成するタスクの手順について説明します。次の手順で行います。

- 1 OVA ファイルをダウンロードします。 [Open Virtualization ファイル](#), (83 ページ) を参照してください。
- 2 VM を作成する (この章)。
- 3 初期設定を実行して、お客様向けに設定します。 [設定](#), (113 ページ) を参照してください。



(注) ゴールデン テンプレートを使用して展開している場合は、この章を省略してください。

Cisco Unified Contact Center Enterprise コール サーバ用の VM の作成

A 側と B 側の CCE コールサーバ用の VM を直接作成するには、次の一連のタスクを実行します。

シーケンス	タスク
1	CCE-PAC-MI-CCE.ova を使用した、 OVA からの仮想マシンの作成 、(85 ページ)。(ドロップダウン リストから [CCE コールサーバ (CCE Call Server)] を選択します)。
2	Windows Server 2008 のインストール 、(89 ページ)
3	Windows での VM の VMware ツールのインストール 、(91 ページ)
4	コールサーバおよびデータサーバのネットワークアダプタの設定 、(91 ページ)
5	Windows アップデートの実行 、(93 ページ)
6	アンチウイルスソフトウェアのインストール 、(88 ページ)
7	Cisco Unified Contact Center Enterprise のインストール 、(98 ページ)
8	宛先システムでの CCE コールサーバの設定。 Cisco Unified CCE コールサーバ 、(127 ページ) を参照してください。

Cisco Unified Contact Center Enterprise データサーバ用の VM の作成

次の手順に従ってタスクを実行し、A 側および B 側で CCE データサーバの仮想マシンを直接作成します。このプロセスは、CCE コールサーバの VM の作成とほぼ同じですが、Microsoft SQL Server をインストールする手順が加わります。

シーケンス	タスク
1	CCE-PAC-MI-CCE.ova を使用した、 OVA からの仮想マシンの作成 、(85 ページ)。ドロップダウン リストから [CCE データベースサーバ (CCE Database Server)] を選択します。
2	Windows Server 2008 のインストール 、(89 ページ)
3	Windows での VM の VMware ツールのインストール 、(91 ページ)
4	コールサーバおよびデータサーバのネットワークアダプタの設定 、(91 ページ)
5	Windows アップデートの実行 、(93 ページ)
6	アンチウイルスソフトウェアのインストール 、(88 ページ)

シーケンス	タスク
7	Microsoft SQL Server のインストール, (93 ページ)
8	Cisco Unified Contact Center Enterprise のインストール, (98 ページ)
9	データベース ドライブの設定, (87 ページ)
10	宛先システムでの CCE データ サーバの VM の設定。 Cisco Unified CCE データ サーバ, (115 ページ) を参照してください。

Cisco Unified Customer Voice Portal サーバ用の VM の作成

Unified CVP コール/VXML サーバおよび Unified CVP OAMP サーバ用の仮想マシンを直接作成するには、次の一連のタスクを実行します。

- Unified CVP コール/VXML サーバが 4 台の仮想マシン (A 側に 2 台および B 側に 2 台) として展開されます。
- Unified CVP OAMP サーバは、A 側の 1 台の仮想マシンとして展開されます。

このプロセスはコール/VXMLおよびOAMPサーバでも同様です。違いは、インストール時にOVAドロップダウンリストから、または[パッケージの選択 (Select Packages)]オプションで選択する内容です。

シーケンス	タスク
1	CCE-PAC-M1-CVP.ova を使用した、 OVA からの仮想マシンの作成, (85 ページ) 。(展開する VM に応じて、ドロップダウンから [CVP OAMP サーバ (CVP OAMP Server)] または [CVP コール サーバ (CVP Call Server)] を選択します)。
2	Windows Server 2008 のインストール, (89 ページ) NTP の設定は、このマシンがコールサーバおよびデータサーバと同じドメインにならない場合に必要です。 NTP および時刻同期, (21 ページ) を参照してください。
3	Windows での VM の VMware ツールのインストール, (91 ページ)
4	Cisco Unified CVP のネットワーク アダプタの設定, (99 ページ)
5	Windows アップデートの実行, (93 ページ)
6	アンチウイルス ソフトウェアのインストール, (88 ページ)
7	Cisco Unified CVP サーバのインストール, (98 ページ)
8	宛先システムでの CVP VM の設定。 Cisco Unified Customer Voice Portal, (141 ページ) を参照してください。

Cisco Unified Communications Manager パブリッシャ用の VM の作成

Cisco Unified Communications Manager パブリッシャ用の仮想マシンを直接作成するには、次の一連のタスクを実行します。

シーケンス	タスク
1	CCE-PAC-M1-CUCM.ova を使用。 OVA からの仮想マシンの作成 、(85 ページ)。(ドロップダウン リストから 7500 ユーザ ノードを選択します)。
2	Cisco Unified Communications Manager パブリッシャのインストール。 VOS ベースのコンタクトセンターアプリケーションのパブリッシャ/プライマリ ノードに対する直接インストール 、(105 ページ) を参照してください。
3	Windows での VM の VMware ツールのインストール 、(91 ページ)
4	Unified Communications Manager の設定。 Cisco Unified Communications Manager 、(157 ページ) を参照してください。

Cisco Unified Communications Manager サブスクライバ用の VM の作成

Cisco Unified Communications Manager サブスクライバ用の仮想マシンを直接作成するには、次の一連のタスクを実行します。

シーケンス	タスク
1	CCE-PAC-M1-CUCM.ova を使用した、 OVA からの仮想マシンの作成 、(85 ページ)。(ドロップダウン リストから 7500 ユーザ ノードを選択します)。
2	Cisco Unified Communications Manager サブスクライバのインストール。 VOS ベースのコンタクトセンターアプリケーションのサブスクライバ/セカンダリ ノードに対する直接インストール 、(109 ページ) を参照してください。
3	Windows での VM の VMware ツールのインストール 、(91 ページ)
4	Unified Communications Manager の設定。 Cisco Unified Communications Manager 、(157 ページ) を参照してください。

Cisco Finesse プライマリ用の VM の作成

A 側の Cisco Finesse プライマリ ノードに直接 VM を作成するには、次の一連の手順を実行します。

シーケンス	タスク
1	CCE-PAC-M1-Finesse.ova を使用した、 OVA からの仮想マシンの作成 、(85 ページ)。(ドロップダウン リストで選択できる項目はありません)。
2	Cisco Finesse プライマリ ノードのインストール。 VOS ベースのコンタクトセンターアプリケーションのパブリッシュ/プライマリ ノードに対する直接インストール 、(105 ページ) を参照してください。
3	Windows での VM の VMware ツールのインストール 、(91 ページ)
4	Cisco Finesse の設定。 Cisco Finesse 、(177 ページ) を参照してください。

Cisco Finesse セカンダリ用の VM の作成

次の手順に従ってタスクを実行し、B 側の Cisco Finesse セカンダリ ノードの仮想マシンを直接作成します。

Cisco Finesse のプライマリ ノードとセカンダリ ノードの VM を作成した後は、それらを設定できます。

シーケンス	タスク
1	CCE-PAC-M1-Finesse.ova を使用した、 OVA からの仮想マシンの作成 、(85 ページ)。(ドロップダウン リストで選択できる項目はありません)。
2	Cisco Finesse セカンダリ ノードのインストール。 VOS ベースのコンタクトセンターアプリケーションのサブスクライバ/セカンダリ ノードに対する直接インストール 、(109 ページ) を参照してください。
3	Windows での VM の VMware ツールのインストール 、(91 ページ)
4	Cisco Finesse の設定。 Cisco Finesse 、(177 ページ) を参照してください。

Cisco Unified Intelligence Center パブリッシャ用の VM の作成

Cisco Unified Intelligence Center パブリッシャ用の仮想マシンを直接作成するには、次の一連のタスクを実行します。

シーケンス	タスク
1	CCE-PAC-M1-CUIC.ova を使用した、 OVA からの仮想マシンの作成 、(85 ページ)。
2	Cisco Unified Intelligence Center パブリッシャのインストール。VOS ベースのコンタクトセンターアプリケーションのパブリッシャ/プライマリ ノードに対する直接インストール、(105 ページ) を参照してください。
3	Windows での VM の VMware ツールのインストール 、(91 ページ)
4	Cisco Unified Intelligence Center の設定。Cisco Unified Intelligence Center、(171 ページ) を参照してください。

Cisco Unified Intelligence Center サブスクライバの VM の作成

Cisco Unified Intelligence Center サブスクライバ用の仮想マシンを直接作成するには、次の一連のタスクを実行します。

シーケンス	タスク
1	CCE-PAC-M1-CUIC.ova を使用した、 OVA からの仮想マシンの作成 、(85 ページ)。
2	Cisco Unified Intelligence Center サブスクライバのインストール。VOS ベースのコンタクトセンターアプリケーションのサブスクライバ/セカンダリ ノードに対する直接インストール、(109 ページ) を参照してください。
3	Windows での VM の VMware ツールのインストール 、(91 ページ)
4	Cisco Unified Intelligence Center の設定。Cisco Unified Intelligence Center、(171 ページ) を参照してください。

Cisco Unified CVP Reporting Server 用の VM の作成

CVP Reporting Server 用の仮想マシンを直接作成するには、次の一連のタスクを実行します。

シーケンス	タスク
1	CCE-PAC-M1-CVP-Reporting.ova を使用した、 OVA からの仮想マシンの作成 、(85 ページ)。 ドロップダウンから [CVP Reporting Server] を選択します。
2	Windows Server 2008 のインストール 、(89 ページ)
3	Windows での VM の VMware ツールのインストール 、(91 ページ)
4	Cisco Unified CVP のネットワーク アダプタの設定 、(99 ページ)
5	Windows アップデートの実行 、(93 ページ)
6	アンチウイルス ソフトウェアのインストール 、(88 ページ)
7	Cisco Unified CVP サーバのインストール 、(98 ページ)
8	データベース ドライブの設定 、(87 ページ)
9	宛先システムでの VM の設定。 Cisco Unified Customer Voice Portal Reporting Server 、(187 ページ) を参照してください。



第 8 章

ゴールデン テンプレートと直接インストール用の共通タスク

- [Open Virtualization ファイル](#), 83 ページ
- [ISO ファイルのマウントおよびアンマウント](#), 83 ページ
- [OVA からの仮想マシンの作成](#), 85 ページ
- [DNS サーバの設定](#), 87 ページ
- [データベース ドライブの設定](#), 87 ページ
- [アンチウイルス ソフトウェアのインストール](#), 88 ページ

Open Virtualization ファイル

Open Virtualization Format ファイルは、CPU、RAM、ディスク容量、CPU の予約、およびメモリの予約を含む作成された VM の基本構造を定義します。

Packaged CCE の OVA ファイルは、Cisco.com にある CCE-PAC-M1-OVA-v10x.zip ファイルに含まれています。

- 1 http://cisco.com/en/US/products/ps12586/tsd_products_support_series_home.html に進みます。[ソフトウェアのダウンロード (Download Software)] をクリックします。[Packaged Contact Center Enterprise 仮想マシンテンプレート (Packaged Contact Center Enterprise Virtual Machine Templates)] を選択します。
- 2 ファイルをダウンロードして解凍し、OVA をローカル ドライブに保存します。

ISO ファイルのマウントおよびアンマウント

データストアに ISO イメージをアップロードします。

- 1 ホストを選択し、[設定 (Configuration)] をクリックします。次に、左側のパネルで [ストレージ (Storage)] をクリックします。
- 2 ISO ファイルを保持するデータストアを選択します。
- 3 [このデータストアを参照 (Browse this datastore)] をクリックします。
- 4 [アップロード (Upload)] アイコンをクリックし、[ファイルのアップロード (Upload file)] を選択します。
- 5 ISO ファイルを保存したローカルドライブの場所を参照し、ISO をデータストアにアップロードします。

ISO イメージをマウントします。

- 1 VM を右クリックし、[仮想マシン設定の編集 (Edit virtual machine settings)] を選択します。
- 2 [ハードウェア (Hardware)] をクリックし、[CD/DVD ドライブ 1 (CD/DVD Drive 1)] を選択します。
- 3 [デバイスのステータス (Device status)] パネル (右上) で [電源投入時に接続 (Connect at Power On)] をオンにします。
- 4 [データストア ISO ファイル (Datastore ISO File)] オプション ボタンをクリックし、[参照 (Browse)] をクリックします。
- 5 ファイルをアップロードするデータストアに移動します。
- 6 [ISO] を選択します。

ISO イメージをアンマウントします。

- 1 VM を右クリックし、[仮想マシン設定の編集 (Edit virtual machine settings)] を選択します。
- 2 [ハードウェア (Hardware)] をクリックし、[CD/DVD ドライブ 1 (CD/DVD Drive 1)] を選択します。
- 3 [デバイスのステータス (Device status)] パネル (右上) で [電源投入時に接続 (Connect at Power On)] をオフにします。

OVA からの仮想マシンの作成

手順

- ステップ 1** vSphere クライアントでホストを選択します。
- ステップ 2** [ファイル (File)] > [OVF テンプレートの展開 (Deploy OVF Template)] を選択します。
- ステップ 3** ローカルドライブ上で OVA が保存されている場所を参照します。[開く (Open)] をクリックしてファイルを選択します。[次へ (Next)] をクリックします。
- ステップ 4** [OVF テンプレートの詳細 (OVF Template Details)] ページで [次へ (Next)] をクリックします。
- ステップ 5** 仮想マシン名を入力します。スペースや特殊文字は使用できません。32 文字以内で入力します。[次へ (Next)] をクリックします。
- ステップ 6** [展開の設定 (Deployment Configuration)] ページで、ドロップダウンを使用して適切な設定を選択します。次に、[次へ (Next)] をクリックします。
- ステップ 7** 新しい仮想マシンを展開するデータストアを選択します。次に、[次へ (Next)] をクリックします。
- 次の表は、各データストアに対して、サーバの RAID グループ、ESXi ホストおよび仮想マシンについて説明します。

C240 M3S の RAID 設定

RAID グループ	VM データストア	ESXi ホスト	仮想マシン
VD0	datastore1	A	ESXi オペレーティングシステム Unified CCE データ サーバ、A 側
VD1	datastore2	A	Unified CCE コール サーバ、A 側 Unified CVP サーバ 1A Unified CVP サーバ 2A Unified Intelligence Center サーバ (パブリッシャ) Unified CVP OAMP サーバ Unified Communications Manager パブリッシャ Unified Communications Manager サブスクリバ 1 Cisco Finesse プライマリ
VD0	datastore1	B	ESXi オペレーティングシステム Unified CCE データ サーバ、B 側

RAID グループ	VM データストア	ESXi ホスト	仮想マシン
VD1	datastore2	B	Unified CCE コール サーバ、B 側 Unified CVP サーバ 1B Unified CVP サーバ 2B Unified Intelligence Center サーバ (サブスクリイバ) Unified Communications Manager サブスクリイバ 2 Unified CVP Reporting Server (任意) Cisco Finesse セカンダリ

ステップ 8 [ディスク フォーマット (Disk Format)] ページでは、デフォルトの仮想ディスク フォーマット ([シック プロビジョニング (Lazy Zeroed) フォーマット (Thick provisioned Lazy Zeroed format)]) のままにします。[次へ (Next)] をクリックします。

ステップ 9 [ネットワーク マッピング (Network Mapping)] ページが CCE コール サーバおよびデータ サーバで正しいことを確認してください。

a) コール サーバおよびデータ サーバの場合 :

- UCCE パブリック ネットワークにパブリックをマッピングする
- UCCE プライベート ネットワークにプライベートをマッピングする

b) 他のすべてのサーバについては、UCCEパブリック ネットワークにパブリックをマッピングする

ステップ 10 「正常に完了しました (Successfully Completed) 」というメッセージが表示されたら、[閉じる (Close)] をクリックします。

DNS サーバの設定

手順

-
- ステップ 1** DNS サーバにログインします。
- ステップ 2** [スタート (Start)] > [管理ツール (Administrative Tools)] > [DNS] を選択します。DNS マネージャが起動されます。
- ステップ 3** [前方参照ゾーン (Forward lookup zone)] で、自動化 Excel シートに入力したドメイン名まで移動します。
- ステップ 4** ドメイン名を右クリックし、[新しいホスト (A または AAAA) (New Host (A or AAAA))] を選択します。
- ステップ 5** [新規ホスト (New Host)] ダイアログボックスで、VOS 製品のコンピュータ名および IP アドレスを入力します。[ホストの追加 (Add Host)] をクリックします。
-

データベース ドライブの設定

手順

-
- ステップ 1** [スタート (Start)] > [すべてのプログラム (All Programs)] > [管理ツール (Administrative Tools)] > [コンピュータの管理 (Computer Management)] を選択します。
- ステップ 2** [ストレージ (Storage)] の下で、[ディスクの管理 (Disk Management)] をクリックします。
- ステップ 3** [ディスクの選択 (Select Disks)] の下の [ディスクの初期化 (Initialize Disk)] ポップアップ ウィンドウで、[ディスク 1 (Disk 1)] をオンにし、[選択したディスクに次のパーティションスタイルを使用する (Use the following partition style for the selected disks)] ペインの下の [MBR (マスターブートレコード) (MBR (Master Boot Record))] を選択します。[OK] をクリックします。
- ステップ 4** 次のように新しいディスク パーティションを作成します。[ディスク 1 (Disk 1)] を右クリックし、[新しいシンプル ボリューム (New Simple Volume)] を選択します。
- デフォルトのボリューム サイズを保持します。[次へ (Next)] をクリックします。
 - ドライブ文字 (E) を割り当てます。[次へ (Next)] をクリックします。
 - NTFS、デフォルトのアロケーション ユニット サイズ、およびボリューム ラベルを選択します。
 - [クイック フォーマットの実行 (Perform a quick format)] オプションをオンにします。[次へ (Next)] をクリックします。
 - [終了 (Finish)] をクリックします。
ステータスが **Healthy** に変わったら、フォーマットは完了です。
-

アンチウイルス ソフトウェアのインストール

サポートされているいずれかのアンチウイルス ソフトウェア製品をインストールします ([サードパーティ製ソフトウェア](#), (7 ページ) を参照)。



重要 自動アップデートを無効にします。アンチウイルス ソフトウェアは手動で更新します。



ヒント インストールプログラム ファイルまたはフォルダに対して必要なアクセスを許可するには、アンチウイルス製品のファイルおよびフォルダ保護ルールでファイルブロックの除外を実行します。McAfee VirusScan でこれを行うには、次の手順を実行します。

- VirusScan コンソールを起動します。
 - [アクセス保護 (Access Protection)] を右クリックし、[プロパティ (Properties)] を選択します。
 - [ウイルス対策標準保護 (Anti-virus Standard Protection)] カテゴリの [ブロック (Block)] 列で、[IRC コミュニケーションをさせない (Prevent IRC communication)] というルールがオフになっていることを確認します。
-



重要 Symantec Endpoint Protection 12.1 のファイアウォール コンポーネントのネットワーク脅威防止機能は、必ずディセーブルにする必要があります。この機能は有効の状態のままで (デフォルト)、デュプレックス ルータの両側がシンプレックス モードで稼働するため、ルータの両側間の通信がブロックされます。このブロックは、すべての導入タイプに影響します。



第 9 章

ゴールデン テンプレートと直接インストール用のソフトウェア インストール

- [Windows Server 2008 のインストール, 89 ページ](#)
- [Microsoft SQL Server のインストール, 93 ページ](#)
- [Cisco Unified Contact Center Enterprise のインストール, 98 ページ](#)
- [Cisco Unified CVP サーバのインストール, 98 ページ](#)
- [Cisco Unified CVP Reporting Server のインストール, 99 ページ](#)
- [データベース ドライブの設定, 101 ページ](#)
- [外部 AW-HDS-DDS のインストールおよび設定, 101 ページ](#)
- [VOS ベースのコンタクト センター アプリケーションに対するゴールデン テンプレートのインストール, 104 ページ](#)
- [VOS ベースのコンタクト センター アプリケーションのパブリッシャ/プライマリ ノードに対する直接インストール, 105 ページ](#)
- [Cisco Unified Communications Manager 用のクラスタの設定, 107 ページ](#)
- [Cisco Unified Communications Manager のサービス構成設定, 108 ページ](#)
- [Cisco Unified Communications Manager パブリッシャのインストール, 108 ページ](#)
- [VOS ベースのコンタクト センター アプリケーションのサブスクリバ/セカンダリ ノードに対する直接インストール, 109 ページ](#)
- [Cisco Unified Intelligence Center 用のクラスタの設定, 111 ページ](#)
- [Cisco Finesse のクラスタの設定, 111 ページ](#)

Windows Server 2008 のインストール

Microsoft Windows Server をインストールするには、次の手順を実行します。

手順

- ステップ 1** Microsoft Windows Server ISO イメージを仮想マシンにマウントします。詳細については、[ISO ファイルのマウントおよびアンマウント](#)、(83 ページ) を参照してください。
- ステップ 2** VM の電源を投入します。
- ステップ 3** [言語 (Language)]、[時刻と通貨の形式 (Time and Currency Format)]、および [キーボード設定 (Keyboard settings)]を入力します。[次へ (Next)]をクリックします。
- ステップ 4** [今すぐインストール (Install Now)]をクリックします。
- ステップ 5** [フルインストール (Full Install)]を選択します。次に、[次へ (Next)]をクリックします。
- ステップ 6** ライセンス条項に同意します。
- ステップ 7** [カスタム (詳細) (Custom (Advanced))]を選択します。次に、[次へ (Next)]をクリックします。インストールが開始されます。
- ステップ 8** インストールの最後に、プロンプトの [OK] をクリックし、ユーザパスワードを入力して確認します。
- ステップ 9** 初期設定タスクの[このサーバのカスタマイズ (Customize This Server)]セクションで、[リモートデスクトップを有効にする (Enable Remote Desktop)]を選択します。
- [スタート (Start)]>[コントロールパネル (Control Panel)]>[システムとセキュリティ (System and Security)]を選択します。
 - [リモートアクセスを許可 (Allow remote access)]をクリックします。
 - 中央のオプション [リモートデスクトップを実行しているコンピュータからの接続を許可する (Allow connections from computers running any version of Remote Desktop)]を選択します。
-

Windows での VM の VMware ツールのインストール

手順

-
- ステップ 1 VM の電源を投入します。
 - ステップ 2 [VM] メニューを右クリックします。[ゲスト (Guest)] > [VMware ツールのインストール/アップグレード (Install / Upgrade VMware tools)] を選択します。
 - ステップ 3 VM コンソールでは、[ソフトウェアとゲームに対して常に実行する (Always do this for software and game)] をオンにします。
 - ステップ 4 **Run setup64.exe** をクリックします。
 - ステップ 5 VMware ツール インストール ウィザードで [次へ (Next)] をクリックします。
 - ステップ 6 デフォルトのセットアップタイプの [標準 (Typical)] を受け入れます。次に、[次へ (Next)] をクリックします。
 - ステップ 7 [インストール (Install)] をクリックします。
 - ステップ 8 再起動を要求されたら、再起動します。
-

コール サーバおよびデータ サーバのネットワーク アダプタの設定

コール サーバおよびデータ サーバには、それぞれ 2 つのネットワーク アダプタが装備されています。MAC アドレスおよびネットワーク ラベルでネットワーク アダプタを特定し、名前を変更し、設定してから、バインディング順序を設定する必要があります。

手順

-
- ステップ 1 次の手順に従って、ネットワーク アダプタの MAC アドレスとラベルを特定します。
 - a) vCenter から、VM を選択し、右クリックします。
 - b) [設定の編集 (Edit Settings)] を選択します。[ハードウェア (Hardware)] タブで、[ネットワーク アダプタ 1 (Network adapter 1)] をクリックします。右側のパネルで、MAC アドレスの最後の数桁を書き留め、ラベルが UCCE パブリックまたは UCCE プライベートかどうかをメモします。たとえば、ネットワーク アダプタ 1 の MAC アドレスは 08-3b で終わり、ネットワーク ラベルが UCCE パブリックである可能性があります。
 - c) ネットワーク アダプタ 2 で繰り返します。MAC アドレスとラベルをメモします。
 - d) VM コンソールで、コマンドラインから **ipconfig /all** と入力します。これはアダプタ名と物理アドレスを表示します。
 - e) アダプタ名と物理アドレスをメモし、VMware でメモした MAC アドレスとラベルと照合します。たとえば、ipconf/all では、ローカルエリア接続 2 の物理アドレスは、08-3b で終了する可能性があります。

- f) VMware が UCCE パブリックとして識別したネットワーク アダプタの MAC アドレスを、ローカルエリア コネクタの対応する物理アドレスと照合します。この例では、ローカルエリア接続 2 (08-3b) の物理アドレスがネットワーク アダプタ 1 の MAC アドレス (o8-3b) に一致します。ローカルエリア接続 2 が UCCE パブリックであることを意味します。

ステップ 2 次のように、Windows のネットワーク アダプタを検索して、名前を変更します。

- a) [ネットワークと共有センター (Network and Sharing Center)] を開き、[ローカルエリア接続 (Local Area Connection)] を選択します。
- b) [ローカルエリア接続 (Local Area Connection)] を右クリックして、[名前の変更 (Rename)] を選択します。上記の照合に応じて、[UCCE Public] または [UCCE Private] に名前を変更します。
- c) [ローカルエリア接続 2 (Local Area Connection 2)] を右クリックして、[名前の変更 (Rename)] を選択します。上記の照合に応じて、[UCCE Public] または [UCCE Private] に名前を変更します。上記の例では、[ローカルエリア接続 2 (Local Area Connection 2)] が UCCE パブリックに名前が変更されます。

ステップ 3 次のように UCCE パブリックのプロパティを設定します。

- a) [UCCE Public] を右クリックし、[プロパティ (Properties)] を選択します。
- b) [ネットワーク (Networking)] ダイアログボックスでは、[インターネットプロトコルバージョン 6 (TCP/IPv6) (Internet Protocol Version 6 (TCP/IPv6))] を選択解除します。
- c) [ネットワーク (Networking)] ダイアログボックスでは、[インターネットプロトコルバージョン 4 (TCP/IPv4) (Internet Protocol Version 4 (TCP/IPv4))] を選択し、[プロパティ (Properties)] を選択します。
- d) インターネットプロトコルバージョン 4 の [全般 (General)] ダイアログボックスで、[次の IP アドレスを使用する (Use the following IP address)] を選択して、IP アドレス、サブネットマスク、デフォルトゲートウェイ、および DNS サーバを入力します。
- e) [OK] と [閉じる (Close)] をクリックして、終了します。

ステップ 4 次のように UCCE プライベートのプロパティを設定します。

- a) [UCCE Private] を右クリックし、[プロパティ (Properties)] を選択します。
- b) [ネットワーク (Networking)] ダイアログボックスでは、[インターネットプロトコルバージョン 6 (TCP/IPv6) (Internet Protocol Version 6 (TCP/IPv6))] を選択解除します。
- c) [ネットワーク (Networking)] ダイアログボックスでは、[インターネットプロトコルバージョン 4 (TCP/IPv4) (Internet Protocol Version 4 (TCP/IPv4))] を選択し、[プロパティ (Properties)] をクリックします。
- d) インターネットプロトコルバージョン 4 の [全般 (General)] ダイアログボックスで、[次の IP アドレスを使用する (Use the following IP address)] を選択して、IP アドレスとサブネットマスクを入力します。
- e) [詳細設定 (Advanced)] をクリックします。[DNS] タブを開きます。[この接続のアドレスを DNS に登録 (Register this connection's addresses in DNS)] をオフにします。
- f) [OK] をクリックして終了します。
- g) c:\windows\system32\drivers\etc に移動し、ホストファイルを編集して、サーバの IP アドレスおよび完全修飾ドメイン名を使用してエントリを追加します。

- h) DNS サーバでは、プライベート IP アドレスのエントリを追加します。この IP のホスト名に *p* などのサフィックスを追加します（プライベートであることを識別するため）。

ステップ 5 バインディング順序は、次のように設定します。

- a) [ネットワーク接続 (Network Connections)] では、Alt キーを押します。次に、[詳細 (Advanced)] > [詳細設定 (Advanced Settings)] を選択します。
- b) [アダプタおよびバインディング (Adapters and Bindings)] ダイアログボックスの上部パネルでは、UCCE パブリック接続が UCCE プライベート接続の上にあることを確認します。正しい順序に並べ替える必要がある場合、矢印ボタンを使用します。[OK] をクリックします。

Windows アップデートの実行

手順

- ステップ 1** Service Pack1 をダウンロードして実行します。
- ステップ 2** 重要な MS Windows アップデートを実行します。アップデートが完了したら、[自動アップデートを有効にしない (Do not enable automatic updates)] をクリックします。
- ステップ 3** <http://support.microsoft.com/kb/2550978> で Windows ホットフィックスを実行します。[Hotfix Download Available] をクリックしたら、プラットフォームタイプが [x64] のホットフィックスを選択します。

Microsoft SQL Server のインストール

Microsoft SQL Server をインストールし、オペレーティングシステムと同じ物理ディスクに SQL Server ログおよびテンポラリ ファイルを保存します（通常は C ドライブ）。

手順

- ステップ 1** Microsoft SQL Server ISO イメージを仮想マシンにマウントします。ISO ファイルのマウントおよびアンマウント、(83 ページ) を参照してください。
- ステップ 2** **setup.exe** を実行します。
- ステップ 3** 左側のペインで [インストール (Installation)] を選択し、[新規インストールを実行するか、既存のインストールに機能を追加する (New installation or add features to an existing installation)] をクリックします。[OK] をクリックします。
- ステップ 4** [プロダクト キー (Product Key)] ページでプロダクト キーを入力し、[次へ (Next)] をクリックします。
- ステップ 5** [ライセンス条項 (License Terms)] に同意し、[次へ (Next)] をクリックします。
- ステップ 6** [セットアップ サポート ルール (Setup Support Rules)] ページで [インストール (Install)] をクリックします。
- ステップ 7** [セットアップ サポート ルール (Setup Support Rules)] ページで [次へ (Next)] をクリックします。
- ステップ 8** [セットアップ ロール (Setup Role)] ページで、[SQL Server 機能のインストール (SQL Server Feature Installation)] を選択します。次に、[次へ (Next)] をクリックします。
- ステップ 9** [機能の選択 (Feature Selection)] ページで、次の内容のみを選択し、[次へ (Next)] をクリックします。
- Database Engine Services
 - Client Tools Connectivity
 - SQL Server Books Online
 - Management Tools - Basic
 - Management Tools - Complete
 - SQL Client Connectivity SDK
- ステップ 10** [インストール ルール (Installation Rules)] ページで [次へ (Next)] をクリックします。
- ステップ 11** [インスタンス設定 (Instance Configuration)] ページで、[既定のインスタンス (Default Instance)] を選択します。[次へ (Next)] をクリックします。
- ステップ 12** [必要なディスク領域 (Disk Space Requirements)] ページで [次へ (Next)] をクリックします。
- ステップ 13** [サーバ設定 (Server Configuration)] ページで [サービス アカウント (Services Account)] タブを選択します。
- a) SQL Server Agent サービスの [アカウント名 (Account Name)] に [NT AUTHORITY\SYSTEM] を選択し、[スタートアップの種類 (Startup Type)] に [自動 (Automatic)] を選択します。
 - b) SQL Server Database Engine サービスの場合、[アカウント名 (Account Name)] に [NT AUTHORITY\SYSTEM] を選択します。
- ステップ 14** [サーバ設定 (Server Configuration)] ページのまま、[照合順序 (Collation)] タブを選択します。

- a) [データベース エンジン (Database Engine)] の [カスタマイズ (Customize)] をクリックします。
- b) [Windows 照合順序指定子と並べ替え順序 (Windows Collation designator and sort order)] オプション ボタンをオンにします。
- c) 適切な照合順序を選択します。通常、カスタマーの組織で最もよく使用される Windows システム ロケールをサポートする SQL Server 照合順序を選択します (たとえば、英語の場合は Latin1_General および Binary など)。
重要: カスタマーの言語表示に適した照合順序の設定を選択することが重要です。インストール時に適切な照合順序を選択しなかった場合、カスタマー側で Microsoft SQL Server をアンインストールしてから再インストールする必要があります。照合順序の設定に関する情報については、この手順の最後にあるリンクを使用してください。

選択する照合順序は、データベースに書き込むことのできる内容に影響します。たとえば、Latin1_General の照合順序を設定した場合に、カスタマー サイトのユーザがサインイン時の言語選択で中国語を選択し、フィールド値を中国語で入力すると、データベースで文字を処理できないため、アプリケーションからサポート対象外の文字であることを示すエラーが戻されます。

- d) [OK] をクリックします。[サーバ設定 (Server Configuration)] ページで [次へ (Next)] をクリックします。

ステップ 15 [データベース エンジン設定 (Database Engine Configuration)] ページで、次を実行します。

- a) [混合モード (Mixed Mode)] をオンにします。
- b) パスワードを入力し、確認のために再入力します。
- c) [現在のユーザの追加 (Add Current User)] をクリックします。
- d) [次へ (Next)] をクリックします。

ステップ 16 [エラー報告 (Error reporting)] ページで [次へ (Next)] をクリックします。

ステップ 17 [インストール設定ルール (Installation Configuration Rules)] ページで [次へ (Next)] をクリックします。

ステップ 18 [インストールの準備完了 (Ready to Install)] ページで [インストール (Install)] をクリックします。

ステップ 19 [完了 (Complete)] ページで [閉じる (Close)] をクリックします。

ステップ 20 SQL Server のサービスパックをインストールします。ウィザードに従い、すべてのデフォルトを受け入れます。

ステップ 21 名前付きパイプをイネーブルにして、次のように並べ替え順序を設定します。

- a) SQL Server Configuration Manager を開きます。
- b) 左側のペインで、[SQL Native Client 10.0 設定 (32 ビット) (SQL Native Client 10.0 Configuration (32 bit))] > [クライアント プロトコル (Client Protocols)] の順に選択します。
- c) 右側のペインで、[名前付きパイプ (Named Pipes)] を右クリックして [有効化 (Enable)] を選択します。
- d) [クライアント プロトコルのプロパティ (Client Protocols Properties)] ウィンドウで [名前付きパイプ (Named Pipes)] を選択し、[上へ移動 (Move Up)] または [下へ移動 (Move down)]

をクリックしてプロトコルを [名前付きパイプ (Named Pipes)]、[TCP/IP] の順に並べ替えて、[OK] をクリックします。

- e) 左側のペインで、[SQL Server ネットワークの設定 (SQL Server Network Configuration)] > [MSSQLSERVER のプロトコル (Protocols for MSSQLSERVER)] の順に選択します。
- f) 右側のペインで、[名前付きパイプ (Named Pipes)] を右クリックして [有効化 (Enable)] を選択します。

ステップ 22 次のように、SQL Server で使用するメモリを予約します。

- a) [SQL Server Management Studio] からサーバを右クリックし、[プロパティ (Properties)] を選択します。
- b) [メモリ (Memory)] をクリックします。
- c) [最大サーバメモリ (MB) (Maximum server memory (in MB))] を 4096 に設定します。

ステップ 23 SQL Server サービスを再起動します。

関連トピック

[ローカリゼーションの照合順序とロケールの設定、\(96 ページ\)](#)

ローカリゼーションの照合順序とロケールの設定

言語の Microsoft SQL Server 照合順序設定

この表は、Packaged CCE および SQL Server の照合順序設定でサポートされている言語をそれぞれ示しています。Microsoft SQL Server 2008 R2 をインストールし、カスタマーの言語表示にマッピングされた照合順序でなければならない場合は、照合順序を選択する必要があります。



メモ 最初の照合順序の選択が誤っている場合、カスタマーは Microsoft SQL Server をアンインストールし、正しい照合順序設定で再インストールする必要があります。

Windows の言語	SQL Server の照合順序設定
英語 デンマーク語 オランダ語 フランス語 ドイツ語 イタリア語 ポルトガル語 (ブラジル) スペイン語 (スペイン) スウェーデン語	Latin1_General
ロシア語	Cyrillic General
中国語 (中国)	Chinese_PRC
中国語 (台湾)	Chinese_Taiwan_Stroke
韓国語	Korean_Wansung
日本語	Japanese

Windows のシステム ロケール

Windows のシステム ロケールが表示言語と一致する必要があります。異なる場合、ユーザ インターフェイスの一部の文字が正しく表示されず、データベースに正しく保存されません。たとえば、システム ロケールが英語で、ユーザがスペイン語で作業している場合、文字鋭アクセント *a* は正しく表示されません。

この手順を両方の CCE コール サーバ、両方の CCE データ サーバ、および任意の外部 HDS システムで実行します。

- 1 [コントロール パネル (Control Panel)] > [地域と言語 (Region and Language)] を開きます。
- 2 [管理 (Administrative)] タブをクリックします。
- 3 [Unicode 対応ではないプログラムの言語 (Language for non-Unicode programs)] で、[システム ロケールの変更 (Change System Locale)] をクリックします。
- 4 言語を選択して、[OK] をクリックします。
- 5 [フォーマット (Format)] タブをクリックします。
- 6 [フォーマット (Format)] では、ステップ 4 で選択した言語を適合させます。
- 7 仮想マシンを再起動します。

Cisco Unified Contact Center Enterprise のインストール

手順

-
- ステップ 1 仮想マシンをドメインに追加します。
 - ステップ 2 Cisco Unified CCE ISO イメージを仮想マシンにマウントします。 [ISO ファイルのマウントおよびアンマウント](#)、(83 ページ) を参照してください。
 - ステップ 3 D:\ICM-CCE-CCH インストーラ ディレクトリから setup.exe を実行します。
 - ステップ 4 InstallShield の手順に従って、Cisco Unified CCE をインストールします。
 - ステップ 5 インストールが完了し、プロンプトが表示されたら、コンピュータを再起動します。
 - ステップ 6 再起動時に、メンテナンスリリースがある場合は、メンテナンスリリースのインストーラが開始されます。
 - ステップ 7 コンピュータを再起動することを要求するプロンプトが表示されたら、[はい (Yes)] をクリックします。次に、[完了 (Finish)] をクリックします。
アプリケーションを直接インストールとして展開している場合は、ステップ 9 に進みます。
 - ステップ 8 ゴールドテンプレートの場合のみ、マシンをドメインから削除し、それをワークグループに追加します。
 - ステップ 9 ISO イメージをアンマウントします。
-

Cisco Unified CVP サーバのインストール

手順

-
- ステップ 1 Unified CVP ISO イメージを仮想マシンにマウントします。詳細については、[ISO ファイルのマウントおよびアンマウント](#)、(83 ページ) を参照してください。
 - ステップ 2 Engineering Special がある場合は、ローカルドライブにコピーします。
 - ステップ 3 D:\CVP\Installer_Windows ディレクトリから setup.exe を実行します。
 - ステップ 4 InstallShield ウィザードに従って、D:\CVP\Installer_Windows ディレクトリから setup.exe を実行します。
 - a) ライセンス契約に同意します。
 - b) [パッケージの選択 (Select Packages)] 画面で、追加するタイプをオンにします。オプションは、[CVP サーバ (CVP Server)]、[Operations Console]、および [Reporting Server] です。
 - c) [次へ (Next)] をクリックします。
 - d) U-Law エンコードされたウェブ形式を選択します。
 - e) [インストール先の選択 (Choose Destination Location)] 画面で、デフォルトを受け入れます。
[次へ (Next)] をクリックします。

- f) [X.509 証明書 (X.509 certificate)] 画面で、証明書に含める情報を入力します。
- g) [インストールの準備完了 (Ready to Install)] 画面で、[インストール (Install)] をクリックします。
- h) OAMP サーバのみの場合、パスワードを入力し、確認します。[次へ (Next)] をクリックします。
- i) [完了 (Finish)] をクリックしてサーバを再起動します。

ステップ 5 Unified CVP のエンジニアリング スペシャルが使用できる場合は、InstallShield ウィザードに従ってそれらをインストールします。

ステップ 6 ISO イメージをアンマウントします。

Cisco Unified CVP のネットワーク アダプタの設定

Unified CVP には、1 つのネットワーク アダプタだけを設定する必要があります。ファイルの名前を変更し、プロパティを設定する必要があります。

手順

- ステップ 1** [スタート (Start)] をクリックします。次に、[コントロール パネル (Control Panel)] をクリックします。
- ステップ 2** [ネットワークと共有センター (Network and Sharing Center)] をクリックします。次に、左側のパネルで [アダプタ設定の変更 (Change adapter settings)] をクリックします。
- ステップ 3** アダプタを右クリックして、[名前の変更 (Rename)] を選択します。その後、UCCE パブリックに名前を変更します。
- ステップ 4** [UCCE Public] を右クリックし、[プロパティ (Properties)] を選択します。
- ステップ 5** [ネットワーク (Networking)] ダイアログボックスでは、[インターネットプロトコルバージョン 6 (TCP/IPv6) (Internet Protocol Version 6 (TCP/IPv6))] を選択解除します。
- ステップ 6** [ネットワーク (Networking)] ダイアログボックスでは、[インターネットプロトコルバージョン 4 (TCP/IPv4) (Internet Protocol Version 4 (TCP/IPv4))] を選択し、[プロパティ (Properties)] を選択します。
- ステップ 7** インターネットプロトコルバージョン 4 の [全般 (General)] ダイアログボックスで、[次の IP アドレスを使用する (Use the following IP address)] を選択して、IP アドレス、サブネットマスク、デフォルト ゲートウェイ、および DNS サーバを入力します。
- ステップ 8** [OK] と [閉じる (Close)] をクリックして、終了します。

Cisco Unified CVP Reporting Server のインストール

このタスクは、オプションの CVP Reporting Server の直接インストールに必要です。

Unified CVP Reporting Server をインストールする前に、データベース ドライブを設定する必要があります（[データベース ドライブの設定](#)、[\(87 ページ\)](#) を参照）。

Unified CVP Reporting Server をインストールするには、次の手順を実行します。

手順

-
- ステップ 1** Unified CVP ISO イメージを仮想マシンにマウントします。詳細については、[ISO ファイルのマウントおよびアンマウント](#)、[\(83 ページ\)](#) を参照してください。
- ステップ 2** 現在のエンジニアリング スペシャルをローカル ドライブにコピーします。
- ステップ 3** DVD ドライブから、CVP\Installer_Windows ディレクトリにある setup.exe を実行します。
- ステップ 4** InstallShield ウィザードに従って、D:\CVP\Installer_Windows ディレクトリから setup.exe を実行します。
- a) ライセンス契約に同意します。
 - b) [パッケージの選択 (Select Packages)] 画面で、[Reporting Server] をオンにします。
 - c) [宛先フォルダの選択 (Choose Destination Folder)] 画面で、CVP インストール フォルダとメディア ファイル インストール フォルダの場所を選択します。
 - d) [X.509 Certificate] 画面に情報を入力します。[次へ (Next)] をクリックします。
 - e) [データベースデータとバックアップドライブの選択 (Choose the database data and backup drive)] 画面で、ドライブ文字（通常は E）を入力します。
 - f) [データベース サイズの選択 (Database size selection)] 画面で、[Premium (375GB)] を選択します。
 - g) [インストールの準備完了 (Ready to Install)] 画面で、[インストール (Install)] をクリックします。
 - h) プロンプトが表示されたら、Reporting Server のパスワードを入力します。
 - i) インストール後にサーバを再起動します。
- ステップ 5** Unified CVP のエンジニアリング スペシャルが使用できる場合は、InstallShield ウィザードに従ってそれらをインストールします。
- ステップ 6** カスタム メディア ファイルを適切な場所に追加します。
- ステップ 7** ISO イメージをアンマウントします。
-

次の作業

導入環境に 2 台目の Unified CVP Reporting Server が必要である場合は、この手順を繰り返します。

データベース ドライブの設定

手順

-
- ステップ 1** [スタート (Start)] > [すべてのプログラム (All Programs)] > [管理ツール (Administrative Tools)] > [コンピュータの管理 (Computer Management)] を選択します。
- ステップ 2** [ストレージ (Storage)] の下で、[ディスクの管理 (Disk Management)] をクリックします。
- ステップ 3** [ディスクの選択 (Select Disks)] に [ディスク 1 (Disk 1)] が表示されたら、オプション [選択したディスクに次のパーティションスタイルを使用する (Use the following partition style for the selected disks)] に [MBR (マスターブートレコード) (MBR (Master Boot Record))] を選択します。
- ステップ 4** [ディスクの選択 (Select Disks)] に [ディスク 1 (Disk 1)] が表示されたら、オプション [選択したディスクに次のパーティションスタイルを使用する (Use the following partition style for the selected disks)] に [MBR (マスターブートレコード) (MBR (Master Boot Record))] を選択します。
- ステップ 5** [ディスクの初期化 (Initialize Disk)] ポップアップで、[ディスク 1 (Disk 1)] を選択し、パーティションスタイルの [MBR (マスターブートレコード) (MBR (Master Boot Record))] を選択します。[OK] をクリックします。
- ステップ 6** 次のように新しいディスク パーティションを作成します。[ディスク 1 (Disk 1)] を右クリックし、[新しいシンプル ボリューム (New Simple Volume)] を選択します。
- デフォルトのボリューム サイズを保持します。[次へ (Next)] をクリックします。
 - ドライブ文字 (E) を割り当てます。[次へ (Next)] をクリックします。
 - NTFS、デフォルトのアロケーション ユニット サイズ、およびボリューム ラベルを選択します。
 - [クイック フォーマットの実行 (Perform a quick format)] オプションをオンにします。[次へ (Next)] をクリックします。
 - [終了 (Finish)] をクリックします。
ステータスが **Healthy** に変わったら、フォーマットは完了です。
-

外部 AW-HDS-DDS のインストールおよび設定

デフォルトの展開では、リアルタイム、履歴およびコール詳細データが保存される CCE データサーバのロガーデータベースからデータが取得されます。履歴データの場合、保持期間は 400 日で、コール詳細データは 40 日です。

より長い保持期間が必要な場合、最大 2 つの別個の外部サーバに、管理サーバ、リアルタイムおよび履歴データサーバ、詳細データサーバ (AW-HDS-DDS) をインストールするオプションが存在します。外部サーバは、[中央コントローラの A 側を優先 (Central Controller Side A Preferred)] または [中央コントローラの B 側を優先 (Central Controller Side B Preferred)] として設定されません。

外部サーバの要件

外部サーバ AW-HDS-DDS の要件については、http://www.cisco.com/en/US/products/sw/custcosw/ps1844/products_implementation_design_guides_list.html で『Cisco Unified Contact Center Enterprise Design Guide』を参照してください。

外部サーバのインストール

- [Windows Server 2008 のインストール](#), (89 ページ)
- [アンチウイルス ソフトウェアのインストール](#), (88 ページ)
- [Microsoft SQL Server のインストール](#), (93 ページ)
- [Cisco Unified Contact Center Enterprise のインストール](#), (98 ページ)。これを行うには、マシンをドメインに追加します。UCCE インストールメディアから `setup.exe` を実行します。終了したら、再起動します。

外部サーバの設定

外部サーバを次のように設定します。

- [SQL Server の設定](#), (115 ページ)
- 保持するデータ量のデータベース ドライブを設定します。
- A 側と B 側の CCE データ サーバのロガーを更新して、[履歴/詳細データの複製を有効にする (Enable Historical/Detail Data Replication)] をオンにします。[Web セットアップのロガー コンポーネントの設定](#), (118 ページ) を参照してください。

外部 AW-HDS-DDS の設定

手順

-
- ステップ 1 [Unified CCE Web セットアップ (Unified CCE Web Setup)] を開きます。
 - ステップ 2 [コンポーネント管理 (Component Management)] > [管理サーバとデータサーバ (Administration & Data Servers)] を選択します。[追加 (Add)] をクリックします。
 - ステップ 3 [展開 (Deployment)] ページで、現在のインスタンスを選択します。
 - ステップ 4 [管理サーバとデータサーバの追加 (Add Administration & Data Servers)] ページで、次のように設定します。
 - a) [エンタープライズ (Enterprise)] をクリックします。
 - b) [小規模から中規模の展開サイズ (Small to Medium Deployment Size)] をクリックします。
 - c) [次へ (Next)] をクリックします。
 - ステップ 5 [小規模から中規模の展開でのサーバロール (Server Role in a Small to Medium Deployment)] ページで、[管理サーバ、リアルタイム/履歴データサーバ、および詳細データサーバ (AW-HDS-DDS)]

(Administration Server Real-time and Historical Data Server, and Detail Data Server (AW-HDS-DDS))] オプションを選択します。[次へ (Next)] をクリックします。

ステップ 6 A 側の [管理 & データ サーバの接続 (Administration & Data Servers Connectivity)] ページで、次の内容を実行します。

- a) [プライマリ管理 & データ サーバ (Primary Administration & Data Server)] のオプション ボタン をクリックします。
- b) [セカンダリ管理 & データ サーバ (*Secondary Administration & Data Server)] フィールドに、そのサーバのホスト名を入力します。
- c) [プライマリ管理 & データ サーバ (*Primary Administration & Data Server)] フィールドに、そのサーバのホスト名を入力します。
- d) [プライマリ/セカンダリ ペア (サイト) 名 (*Primary/Secondary Pair (Site) Name)] フィールド に CCE-AW-1 を入力します。
- e) [次へ (Next)] をクリックします。

または、B 側の [管理 & データ サーバの接続 (Administration & Data Servers Connectivity)] ページで、次の内容を実行します。

- a) [プライマリ管理 & データ サーバ (Primary Administration & Data Server)] のオプション ボタン をクリックします。
Packaged CCE の場合、すべての AW HDS DDS がプライマリです。
- b) [セカンダリ管理 & データ サーバ (*Secondary Administration & Data Server)] フィールドに、そのサーバのホスト名を入力します。
- c) [プライマリ管理 & データ サーバ (*Primary Administration & Data Server)] フィールドに、そのサーバのホスト名を入力します。
- d) [プライマリ/セカンダリ ペア (サイト) 名 (*Primary/Secondary Pair (Site) Name)] フィールド に CCE-AW-2 を入力します。
- e) [次へ (Next)] をクリックします。

ステップ 7 [データベースとオプション (Database and Options)] ページで、次のように設定します。

- a) [次のドライブ上でデータベースを作成 (Create Database(s) on Drive)] フィールドで、[C] を選択します。
- b) [エージェントのスキル変更 (Agent Re-skilling)] Web ツールをクリックしないでください。
Packaged CCE ではこのツールはサポートされていません。スーパーバイザは、エージェント ツール上のユーザ インターフェイスでエージェントのスキルを変更します。
- c) [Internet Script Editor] をクリックします。
- d) [次へ (Next)] をクリックします。

ステップ 8 [セントラル コントローラの接続 (Central Controller Connectivity)] ページで、次のように設定します。

- a) ルータ A 側には、Unified CCE コール サーバ A の IP アドレスを入力します。
- b) ルータ B 側には、Unified CCE コール サーバ B の IP アドレスを入力します。
- c) ロガー A 側には、Unified CCE データ サーバ A の IP アドレスを入力します。
- d) ロガー B 側には、Unified CCE データ サーバ B の IP アドレスを入力します。
- e) [セントラル コントローラ ドメイン名 (Central Controller Domain Name)] を入力します。

- f) [中央コントローラの A 側を優先 (Central Controller Side A Preferred)]または[中央コントローラの B 側を優先 (Central Controller Side B Preferred)]をクリックします。
- g) [次へ (Next)]をクリックします。

ステップ 9 [サマリー (Summary)] ページの内容を確認してから、[完了 (Finish)] をクリックします。

外部 AW-HDS-DDS の HDS データベースの作成

ICMDBA を使用して HDS データベースを作成します。

手順

-
- ステップ 1** [スタート (Start)] > [すべてのプログラム (All Programs)] > [Cisco Unified CCE ツール (Cisco Unified CCE Tools)] > [ICMdba] を選択します。警告が表示されたら [はい (Yes)] をクリックします。
 - ステップ 2** [管理 & データ サーバ (Administration & Data Server)] の下にデータベースが表示されるまで、インスタンスのツリー ビューを展開します。
 - ステップ 3** [管理 & データ サーバ (Administration & Data Server)] を選択します。
 - ステップ 4** メニューから、[データベース (Database)] > [作成 (Create)] の順に選択します。次に、[追加 (Add)] をクリックします。
 - ステップ 5** [データ (Data)] オプション ボタンをクリックし、2 番目のディスク ドライブを選択し、目的の HDS のサイズを入力します。[OK] をクリックします。
 - ステップ 6** [ログ (Log)] オプション ボタンをクリックし、2 番目のディスク ドライブを選択し、目的のログサイズを入力します。[OK] をクリックします。
 - ステップ 7** [作成 (Create)] をクリックします。
-

VOS ベースのコンタクトセンターアプリケーションに対するゴールデンテンプレートのインストール

VOS ベースのコンタクト センター アプリケーションに対してゴールドテンプレートを作成するには、次の手順を実行します。

手順

- ステップ 1** ISO ファイルを仮想マシンの CD/DVD ドライブにマウントします。詳細については、[ISO ファイルのマウントおよびアンマウント](#)、(83 ページ) を参照してください。
- ステップ 2** 仮想マシンを選択して、電源をオンにします。次に、コンソールを開きます。
- ステップ 3** インストール ウィザードを実行します。
- [Media Check Result/Success] 画面で、[Yes] を選択します。
 - [Product Deployment Selection] 画面で、[Yes] を選択します。
 - [インストールの続行 (Proceed with Install)] 画面で、[はい (Yes)] を選択します。
 - [プラットフォームのインストール (Platform Installation)] 画面で、[スキップ (Skip)] を選択します。
開始から約 10 分後、コンポーネントのインストールが完了するとリポートが行われます。
 - リポート後に、[Pre-existing Configuration Information] 画面で、[Continue] をクリックします。
 - [Platform Installation Wizard] で、[Cancel] を選択して、インストールをキャンセルします。[OK] をクリックして、システムを停止します。
 - Ctrl+Alt を押してカーソルを解放します。ただちに、画面の左上にある赤い [シャットダウン (Shut Down)] アイコンをクリックします。
 - ISO イメージをアンマウントします。

VOS ベースのコンタクトセンターアプリケーションのパブリッシャ/プライマリノードに対する直接インストール

このタスクは、VOS ベースの 3 つのコンタクトセンターアプリケーション (Cisco Finesse、Cisco Unified Communications Manager、および Cisco Unified Intelligence Center) のパブリッシャ/プライマリノードに必要です。ゴールデンテンプレートを作成するために、この手順を使用しないでください。

インストールでは、コマンドラインインターフェイスを使用します。Tab キーを使用してオプションに移動し、Enter キーで選択します。

はじめる前に

DNS 設定は、Cisco Unified Communications Manager、Cisco Unified Intelligence Center、および Cisco Finesse のインストールに必須です。DNS を設定するには、VM を DNS の前方および逆引き参照に追加します。[DNS サーバの設定](#)、(87 ページ) を参照してください。

手順

- ステップ 1 VM を右クリックして、[設定の編集 (Edit Settings)] を選択します。
- ステップ 2 [ハードウェア (Hardware)] をクリックし、[CD|DVD ドライブ 1 (CD|DVD Drive 1)] を選択します。
- ステップ 3 [接続済み (Connected)] と [パワーオン時に接続 (Connect at power)] チェックボックスが両方ともオンになっていることを確認します (右上の [デバイスのステータス (Device status)] パネル)。
- ステップ 4 仮想マシンを選択して、電源をオンにします。
- ステップ 5 インストール ウィザードに従い、次のように選択します。
 - a) [DVD が見つかりました (DVD Found)] 画面で、[はい (Yes)] をクリックして、メディアの整合性確認を始めます。
 - b) [メディア チェック結果 (Media Check Results)] 画面で、[OK] を選択します。
 - c) [製品展開の選択 (Product Deployment Selection)] 画面で、[OK] を選択します。
 - d) [インストールの続行 (Proceed with Install)] 画面で、[はい (Yes)] を選択します。
 - e) [プラットフォームのインストール ウィザード (Platform Installation Wizard)] 画面で、[続行 (Proceed)] を選択します。
 - f) [パッチの適用 (Apply Patch)] 画面で、[いいえ (No)] を選択します。
 - g) [基本インストール (Basic Install)] 画面で、[続行 (Continue)] を選択します。
 - h) [タイムゾーンの設定 (Timezone Configuration)] 画面で、下矢印を使用して、サーバが配置されている場所に最も近い現地のタイムゾーンを選択します。[OK] を選択します。
 - i) [自動ネゴシエーションの設定 (Auto Negotiation Configuration)] 画面で、[はい (Yes)] を選択します。
 - j) [MTU の設定 (MTU Configuration)] 画面で [いいえ (No)] を選択して、最大伝送単位をデフォルト設定 (1500) のままにします。
 - k) [DHCP の設定 (DHCP Configuration)] 画面で、[いいえ (No)] を選択します。(Finesse にはこの手順はありません)。
 - l) [スタティック ネットワーク設定 (Static Network Configuration)] 画面で、静的設定値を入力します。[OK] を選択します。
 - m) [DNS クライアントの設定 (DNS Client Configuration)] 画面で、[はい (Yes)] を選択します。
 - n) DNS クライアントの設定を入力します。[OK] を選択します。
 - o) [管理者ログインの設定 (Administrator Login Configuration)] 画面で、システム管理者の ID を入力します。管理者のパスワードを入力して確認します。[OK] を選択します。
 - p) [証明書情報 (Certificate Information)] 画面で、証明書署名要求を作成するためのデータ (組織、部門、場所、都道府県、国) を入力します。[OK] を選択します。
 - q) [最初のノード設定 (First Node Configuration)] 画面で、[はい (Yes)] を選択します。[OK] をクリックします。
 - r) [ネットワーク タイム プロトコル クライアントの設定 (Network Time Protocol Client Configuration)] 画面で、有効な NTP サーバの IP アドレスを入力し、[OK] を選択します。入力する正しい NTP サーバ情報を判別するには、[NTP および時刻同期](#)、(21 ページ) を参照してください。適切な NTP の設定が必要です。

- s) [セキュリティの設定 (Security Configuration)] 画面で、セキュリティ パスワードを入力し、[OK] を選択します。
- t) [SMTP ホストの設定 (SMTP Host Configuration)] 画面で、[いいえ (No)] を選択します。
(Finesse にはこの手順はありません)。
- u) [アプリケーションユーザの設定 (Application User Configuration)] 画面で、アプリケーション ユーザ名を入力し、アプリケーションユーザパスワードを入力して確認します。[OK] を選択します。
- v) [プラットフォーム設定の確認 (Platform Configuration Confirmation)] 画面で、[OK] を選択します。インストールが始まり、自動で実行されます。
- w)
 - インストールの途中でリブートが行われます。
 - ライセンスを取得するための URL
(<https://tools.cisco.com/SWIFT/Licensing/PrivateRegistrationServlet>) とメディアアクセス コントロール (MAC) アドレスを示す [製品ライセンス (Product Licensing)] 画面が表示された場合は、このアドレスを書き留めます。このアドレスは、ライセンスの申請で必要になります。
 - インストールが終了し、ログインプロンプトが表示されます。

次の作業



- メモ** Finesse に対してのみ、ノードのインストール後に Cisco Security Agent (CSA) を無効にする必要があります。これを行うには、B 側の Finesse VM から、コマンドラインインターフェイスにアクセスし、コマンド **utils csa disable** を入力します。プロンプトに従ってリブートします。

Cisco Unified Communications Manager 用のクラスタの設定

手順

- ステップ 1** ブラウザで Unified Communications Manager パブリッシャを起動します (<http://<IP Addr of CUCM Publisher>>)。
- ステップ 2** [システム (System)] > [サーバ (Server)] > [新規追加 (Add New)] を選択します。
- ステップ 3** [サーバの設定 (Server Configuration)] タブで、サブスクライバの IP アドレスを入力します。
- ステップ 4** [保存 (Save)] をクリックします。

Cisco Unified Communications Manager のサービス構成設定

ロケーションベースのコールアドミッション制御（CAC）は、Unified CCE 支社コールフローモデル（別名、集中型モデル）で使用されます。これは、すべてのサーバ（Unified CVP、Unified CCE、Unified Communications Manager、および SIP プロキシサーバ）が 1 つまたは 2 つのデータセンターおよびそれぞれの支社に集中化されることを意味します。

次の設定パラメータを設定して、Unified Communications Manager がコールの発信ロケーションとしての Unified CVP ではなく、入力ゲートウェイを使用するようにします。これらの設定により、CAC が発信側エンドポイントと電話機の場所に基づいて適切に調整されます。

手順

-
- ステップ 1 Unified CM サービスパラメータの [不明な TCP 接続を受け入れる (Accept Unknown TCP connection)] を設定します。
 - ステップ 2 Unified CM サービスパラメータの [1720 をリッスンする GK 制御トランク (GK controlled trunk that will listen to 1720)] を [なし (None)] に設定します。
 - ステップ 3 Unified CM のゲートウェイデバイスとして Unified CVP を定義しないでください。
 - ステップ 4 Unified CM のゲートウェイデバイスとして入力ゲートウェイを定義します。デバイスに正しい場所を割り当てます。
-

Cisco Unified Communications Manager パブリッシャのインストール

Cisco Unified Communications Manager パブリッシャは、「Component Software」セクションに記載されている Linux ベースの Unified Communications オペレーティングシステムにインストールされています。ここをクリックして、[VOS ベースのコンタクトセンターアプリケーションに対するゴールデンテンプレートのインストール](#)、(104 ページ)に進みます。完了したら、このページに戻って、一連のタスクを続行します。

VOS ベースのコンタクトセンターアプリケーションのサブスライバ/セカンダリノードに対する直接インストール



(注) このタスクは、VOS ベースの 3 つのコンタクトセンターアプリケーション (Cisco Finesse、Cisco Unified Communications Manager、および Cisco Unified Intelligence Center) のサブスライバ/セカンダリノードに必要です。ゴールデンテンプレートを作成するために、この手順を使用しないでください。

サブスライバ/セカンダリノードをインストールするには、まず、パブリッシャ/プライマリノードをインストールし、クラスタを設定する必要があります。 [VOS ベースのコンタクトセンターアプリケーションのパブリッシャ/プライマリノードに対する直接インストール](#)、(105 ページ)

はじめる前に

Cisco Unified Communications Manager、Cisco Unified Intelligence Center、および Cisco Finesse 用の DNS 設定が必須です。DNS を設定するには、VM を DNS の前方および逆引き参照に追加します。 [DNS サーバの設定](#)、(87 ページ) を参照してください。

手順

- ステップ 1 VM を右クリックして、[設定の編集 (Edit Settings)] を選択します。
- ステップ 2 [ハードウェア (Hardware)] をクリックし、[CD|DVD ドライブ 1 (CD|DVD Drive 1)] を選択します。
- ステップ 3 [接続済み (Connected)] と [パワーオン時に接続 (Connect at power)] チェックボックスが両方ともオンになっていることを確認します (右上の [デバイスのステータス (Device status)] パネル)。
- ステップ 4 仮想マシンを選択して、電源をオンにします。
- ステップ 5 インストールウィザードに従い、次のように選択します。
 - a) [DVD が見つかりました (DVD Found)] 画面で、[はい (Yes)] をクリックして、メディアの整合性確認を始めます。
 - b) [メディアチェック結果 (Media Check Results)] 画面で、[OK] を選択します。
 - c) [製品展開の選択 (Product Deployment Selection)] 画面で、[OK] を選択します。
 - d) [インストールの続行 (Proceed with Install)] 画面で、[はい (Yes)] を選択します。
 - e) [プラットフォームのインストールウィザード (Platform Installation Wizard)] 画面で、[続行 (Proceed)] を選択します。
 - f) [パッチの適用 (Apply Patch)] 画面で、[いいえ (No)] を選択します。
 - g) [基本インストール (Basic Install)] 画面で、[続行 (Continue)] を選択します。
 - h) [タイムゾーンの設定 (Timezone Configuration)] 画面で、下矢印を使用して、サーバが配置されている場所に最も近い現地のタイムゾーンを選択します。[OK] を選択します。

- i) [自動ネゴシエーションの設定 (Auto Negotiation Configuration)]画面で、[はい (Yes)]を選択します。
- j) [MTU の設定 (MTU Configuration)]画面で [いいえ (No)]を選択して、最大伝送単位をデフォルト設定 (1500) のままにします。
- k) [DHCP の設定 (DHCP Configuration)]画面で、[いいえ (No)]を選択します。
- l) [スタティックネットワーク設定 (Static Network Configuration)]画面で、静的設定値を入力します。[OK] を選択します。
- m) [DNS クライアントの設定 (DNS Client Configuration)]画面で、[はい (Yes)]を選択します。
- n) DNS クライアントの設定を入力します。[OK] を選択します。
- o) [管理者ログインの設定 (Administrator Login Configuration)]画面で、システム管理者の ID を入力します。管理者のパスワードを入力して確認します。[OK] を選択します。
- p) [証明書情報 (Certificate Information)]画面で、証明書署名要求を作成するためのデータ (組織、部門、場所、都道府県、国) を入力します。[OK] を選択します。
- q) [最初のノード設定 (First Node Configuration)]画面で、[いいえ (No)]を選択します。[OK] を選択します。
警告画面が表示され、最初のノードへのネットワーク接続を確認することが要求されます。
- r) [プラットフォーム設定の確認 (Platform Configuration Confirmation)]画面で、[OK] を選択します。インストールが始まり、自動で実行されます。
- s)
 - インストールの途中でリブートが行われます。
 - ライセンスを取得するための URL
(<https://tools.cisco.com/SWIFT/Licensing/PrivateRegistrationServlet>) とメディアアクセスコントロール (MAC) アドレスを示す [製品ライセンス (Product Licensing)]画面が表示されたら、このアドレスを書き留めます。このアドレスは、ライセンスの申請に必要になります。
 - インストールが終了し、ログインプロンプトが表示されます。

次の作業



メモ

Finesse に対してのみ、ノードのインストール後に Cisco Security Agent (CSA) を無効にする必要があります。これを行うには、B 側の Finesse VM から、コマンドラインインターフェイスにアクセスし、コマンド **utils csa disable** を入力します。プロンプトに従ってリブートします。

Cisco Unified Intelligence Center 用のクラスタの設定

手順

-
- ステップ 1 ブラウザで URL `http://<HOST ADDRESS>/oamp` にアクセスします。ここで、HOST ADDRESS は Cisco Unified Intelligence Center パブリッシャの IP アドレスまたはホスト名です。
 - ステップ 2 インストール時に定義したシステム アプリケーション ユーザ ID とパスワードを使用してサインインします。
 - ステップ 3 左のパネルから、[デバイス管理 (Device Management)] > [デバイス設定 (Device Configuration)] を選択します。
 - ステップ 4 [メンバーの追加 (Add Member)] をクリックします。
 - ステップ 5 サブスクリバ用の [デバイス設定 (Device Configuration)] の各フィールドに、デバイスの名前、ホスト名または IP アドレス、および説明を入力します。
-

Cisco Finesse のクラスタの設定

手順

-
- ステップ 1 ブラウザで Cisco Finesse プライマリ ノードを起動します (`http://Primary Node IP Address/cfadmin`)。ここで、Primary Node または IP Address は自分のホストのプライマリ ノードまたは IP アドレスです。
 - ステップ 2 [ホーム (Home)] > [クラスタの設定 (Cluster Settings)] に移動します。(これは、デフォルト設定に基づいており、クラスタ設定ガジェットのパージを変更していないことが前提となります)。
 - ステップ 3 Cisco Finesse セカンダリ ノードの IP アドレスを追加します。
 - ステップ 4 [送信 (Submit)] をクリックします。
-



第 **III** 部

設定

- [Cisco Unified CCE データ サーバ, 115 ページ](#)
- [Cisco Unified CCE コール サーバ, 127 ページ](#)
- [Cisco Unified Customer Voice Portal, 141 ページ](#)
- [Cisco IOS Enterprise 音声ゲートウェイの設定, 151 ページ](#)
- [Cisco Unified Communications Manager, 157 ページ](#)
- [展開タイプの設定, 169 ページ](#)
- [Cisco Unified Intelligence Center, 171 ページ](#)
- [Cisco Finesse, 177 ページ](#)
- [Cisco Unified Customer Voice Portal Reporting Server, 187 ページ](#)



第 10 章

Cisco Unified CCE データ サーバ

この章には、A 側と B 側の Unified CCE データ サーバに対して実行する必要がある設定手順が含まれます。

- [SQL Server の設定, 115 ページ](#)
- [ドメイン マネージャの設定, 116 ページ](#)
- [インスタンスのセットアップ, 117 ページ](#)
- [ロガーの設定, 117 ページ](#)
- [ロガー データベースおよびログの設定, 117 ページ](#)
- [Web セットアップのロガー コンポーネントの設定, 118 ページ](#)
- [基本設定の適用, 119 ページ](#)
- [ICMDBA ツールを使用した基本設定の実行, 120 ページ](#)
- [AW データベースおよびログの設定, 122 ページ](#)
- [管理サーバおよびリアルタイム データ サーバのコンポーネントの設定, 123 ページ](#)
- [Unified Intelligence Center の SQL ユーザ アカウントの設定, 124 ページ](#)

SQL Server の設定

手順

- ステップ 1** [スタート (Start)]>[すべてのプログラム (All Programs)]>[Microsoft SQL Server 2008 R2]>[SQL Server Management Studio] に移動します。
- ステップ 2** ログインします。
- ステップ 3** [セキュリティ (Security)] と [ログイン (Logins)] を順に展開します。
- ステップ 4** BUILTIN \ Administrator グループが表示されていない場合:

- a) [ログイン (Logins)] を右クリックし、[新しいログイン (New Login)] を選択します。
 - b) [検索 (Search)] をクリックし、[場所 (Locations)] を選択して、ドメインツリー内の BUILTIN の場所を見つけます。
 - c) **Administrators** と入力し、[名前の確認 (Check Name)] をクリックし、[OK] をクリックします。
 - d) [BUILTIN\Administrators] をダブルクリックします。
 - e) [サーバロール (Server Roles)] を選択します。
 - f) [public] と [sysadmin] が両方ともオンになっていることを確認します。
-

ドメインマネージャの設定

この作業は一度だけ（設定する最初の Unified データ サーバ上で）行います。

手順

- ステップ 1** [スタート (Start)] > [すべてのプログラム (All Programs)] > [Cisco Unified CCE ツール (Cisco Unified CCE Tools)] > [ドメインマネージャ (Domain Manager)] を選択します。
 - ステップ 2** ドメインに OU を作成する権限を持つユーザとしてログインします。
 - ステップ 3** 左側のペインで、ドメインを展開します。
 - ステップ 4** Cisco_ICM、として Cisco Root を追加します。
 - a) [Cisco root] の下の、[追加 (Add)] をクリックします。
 - b) Cisco Root OU を下に作成する組織単位 (OU) を選択します。[OK] をクリックします。
 - ステップ 5** ファシリティ組織単位 (OU) を追加します。
 - a) 右側のペインの [ファシリティ (Facility)] の下で、[追加 (Add)] をクリックします。
 - b) ファシリティの名前を入力します。[OK] をクリックします。
 - ステップ 6** インスタンス OU を追加します。
 - a) 右側のペインの [インスタンス (Instance)] の下で、[追加 (Add)] をクリックします。
 - b) インスタンス名を入力し、[OK] をクリックします。
 - ステップ 7** [閉じる (Close)] をクリックします。
-

インスタンスのセットアップ

手順

-
- ステップ 1 [Unified CCE Web セットアップ (Unified CCE Web Setup)] を起動します。
 - ステップ 2 ローカルの管理者権限を持つドメイン ユーザを使用してサインインします。
 - ステップ 3 [インスタンス管理 (Instance Management)] をクリックし、[追加 (Add)] をクリックします。
 - ステップ 4 [インスタンスの追加 (Add Instance)] ページで、次のように設定します。
 - a) ファシリティとインスタンスを選択します。
 - b) [インスタンス番号 (Instance Number)] フィールドに 0 と入力します。
 - ステップ 5 [保存 (Save)] をクリックします。
-

ロガーの設定

ロガー データベースおよびログの設定

手順

-
- ステップ 1 [スタート (Start)] > [すべてのプログラム (All Programs)] > [Cisco Unified CCE ツール (Cisco Unified CCE Tools)] > [ICMdba] を選択します。警告が表示されたら、[はい (Yes)] をクリックして、閉じます。
 - ステップ 2 [サーバ (Server)] > [インスタンス (Instance)] に移動します。
 - ステップ 3 インスタンス名を右クリックし、[作成 (Create)] を選択します。
 - ステップ 4 [コンポーネントの選択 (Select Component)] ダイアログボックスで、作業中のロガー ([ロガー A (Logger A)] または [ロガー B (Logger B)]) を選択します。[OK] をクリックします。
 - ステップ 5 プロンプト [SQL Server is not configured properly. Do you want to configure it now?] で、[はい (Yes)] をクリックします。
 - ステップ 6 [設定 (Configure)] ページで、[SQL Server 設定 (SQL Server Configurations)] ペイン内の [メモリ (MB) (Memory (MB))] と [リカバリ間隔 (Recovery Interval)] のデフォルトを確認します。[OK] をクリックします。
 - ステップ 7 [サーバの停止 (Stop Server)] ページで、[はい (Yes)] をクリックしてサービスを停止します。
 - ステップ 8 [ロガー タイプの選択 (Select Logger Type)] ダイアログボックスで、[エンタープライズ (Enterprise)] を選択します。[OK] をクリックして、[データベースの作成 (Create Database)] ダイアログボックスを開きます。
 - ステップ 9 ロガーのデータベースを作成し、次のようにログを作成します。

- a) [DB タイプ (DB Type)]フィールドで、側 (A または B) を選択します。
- b) [ストレージ (Storage)]ペインで、[追加 (Add)]をクリックします。
- c) [データ (Data)]をクリックします
- d) E ドライブを選択します。
- e) [サイズ (Size)]フィールドに 665600 MB と入力します。
- f) [OK] をクリックして、[データベースの作成 (Create Database)]ダイアログボックスに戻ります。
- g) [追加 (Add)]を再度クリックします。
- h) E ドライブを選択します。
- i) [サイズ (Size)]フィールドに 3072MB と入力します。
- j) [OK] をクリックして、[データベースの作成 (Create Database)]ダイアログボックスに戻ります。

ステップ 10 [データベースの作成 (Create Database)]ダイアログボックスで、[作成 (Create)]をクリックします。[開始 (Start)]をクリックします。
作成の成功メッセージが表示されたら、[OK] と [閉じる (Close)]を順にクリックします。

Web セットアップのロガー コンポーネントの設定

手順

- ステップ 1** ロガー コンポーネントを次のように設定します。
- a) [Unified CCE Web セットアップ (Unified CCE Web Setup)]に戻ります。再度ログインしなければならない場合があります。
 - b) [コンポーネント管理 (Component Management)]>[ロガー (Loggers)]を選択します。[追加 (Add)]をクリックします。インスタンスを選択します。
 - c) [展開 (Deployment)]ページで、[デュプレックス (Duplexed)]をクリックします。[次へ (Next)]をクリックします。
 - d) [セントラル コントローラの接続 (Central Controller Connectivity)]ページで、ルータ プライベート インターフェイスとロガー プライベート インターフェイスについて A 側と B 側のホスト名を入力します。
 - e) [次へ (Next)]をクリックします。
- ステップ 2** [追加オプション (Additional Options)]ページで、次の内容を実行します。
- a) 展開内に外部 AW-HDS-DDS が存在する場合は、[履歴/詳細データの複製を有効にする (Enable Historical/Detail Data Replication)]をオンにします。
 - b) [データベースの消去設定手順の表示 (Display Database Purge Configuration Step)]をオンにします。

- c) [次へ (Next)] をクリックします。
- ステップ 3** [データ保持 (Data Retention)] ページで、[データベース保持設定 (Database Retention Configuration)] テーブルを変更します。
- a) 次のテーブルでは、保持時間を「40」に設定します。
- Application_Event
 - Event
 - Network_Event
 - Route_Call_Detail
 - Route_Call_Variable
 - Termination_Call_Detail
 - Termination_Call_Variable
- b) その他すべてのテーブルに対して保持期間を 400 日に設定します。
- c) [次へ (Next)] をクリックします。
- ステップ 4** [データの消去 (Data Purge)] ページで、システム上で需要が低いときの曜日と時間の消去を設定します。
- ステップ 5** デフォルトの [上限 (%) に達した場合は自動で消去する (Automatic Purge at Percent Full)] を受け入れます。
- ステップ 6** [次へ (Next)] をクリックします。
- ステップ 7** [サマリー (Summary)] ページの内容を確認してから、[完了 (Finish)] をクリックします。

基本設定の適用

基本設定について

基本構成は、システムの次の機能を実行します。

Packaged CCE のコール ルーティングおよびダイヤル プランをサポートするコア システム オブジェクトを作成します。

2 つの Peripheral Gateway を作成します。

- 1 つの CUCM PIM と 4 つの CVP PIM を使用する汎用 PG
- 2 つの PIM (アウトバウンド用に 1 つ、マルチチャネル用に 1 つ) を使用する MR PG

Packaged CCE 展開モデルのインテリジェント アプリケーション デフォルトを設定します。

- デフォルトのエージェント デスク設定レコード
- ECC 変数の有効化

CVP をサポートする設定オブジェクトを作成します。

- CVP 用のタイプ 10 ネットワーク VRU および CVP にコールを送信するネットワーク VRU ラベル
- CVP ECC 変数
- VXML_Server ネットワーク VRU スクリプト (GS、V microapp)

マルチチャネル設定をサポートする設定オブジェクトを作成します。

- MR PG のネットワーク VRU
- マルチチャネルのアプリケーション インスタンス
- マルチチャネルのメディア クラス

新規インストールのみに基本設定を適用

基本設定は、Packaged CCE の新規インストール時に 1 回実行されます。基本設定が Packaged CCE にすでに適用されており、Packaged CCE の最新リリースにアップグレードする場合、基本設定の 2 回目のダウンロードは行わないでください。このような場合は、設定変更を手動で適用します。

関連トピック

[基本設定の更新](#)、(223 ページ)

ICMDBA ツールを使用した基本設定の実行

このタスクは、フレッシュインストールに必要です。この手順は、A 側の CCE データ サーバで実行します。

手順

-
- ステップ 1** Cisco.com>[ソフトウェアダウンロード (Download Software)]>[Packaged Contact Center Enterprise Configuration Scripts] (<http://software.cisco.com/download/type.html?mdfid=284360381&i=rm>) から基本設定用の zip ファイルをダウンロードします。このファイルをローカルに保存し、解凍します。
- ステップ 2** 同じ場所から *Domain_Update_Tool.zip* ファイルをダウンロードします。このファイルをローカルに保存し、解凍します。
- ステップ 3** A 側の CCE データ サーバで ICMDBA ツールを開きます。
- ステップ 4** [CCE データ サーバ (CCE Data Server)] を選択し、<instance name>_sideA までツリーを展開します。
- ステップ 5** メニューバーの [データ (Data)] を選択し、[インポート (Import)] をクリックします。
- ステップ 6** 設定フォルダを参照して特定し、[開く (Open)] をクリックします。
- ステップ 7** [OK] をクリックしてから、[インポート (Import)] をクリックします。
- ステップ 8** [開始 (Start)] をクリックし、すべてのメッセージに対して [OK] をクリックします。
- ステップ 9** **Domain_Update_Tool** フォルダに移動し、[UpdateDomain.PS1] を右クリックして、[PowerShell で実行する (Run with PowerShell)] を選択します。次のように応答します。
- サーバ名として、A 側の CCE データ サーバのコンピュータ名を入力します。
 - データベース名として、<instance_sideA> と入力します。
 - ドメイン名として、カスタマーのドメイン名を入力します。
- ステップ 10** ICMDBA ツールに戻ります。
- ロガー データベース (<instance_sideA>) をクリックします。
 - メニューバーの [データ (Data)] を開き、[同期 (Synchronize)] をクリックします。
 - [ターゲット ペイン (Target Pane)] の下で、[B 側の CCE データ サーバ (CCE Data Server on Side B)] を選択します。
 - データベース名としてターゲット側の <instance name>_sideB を入力します。
 - [同期 (Synchronize)] をクリックします。
- ステップ 11** [開始 (Start)] をクリックします。
- ステップ 12** すべてのメッセージに対して、[はい (Yes)] をクリックします。
- ステップ 13** [閉じる (Close)] をクリックします。
-

AW データベースおよびログの設定

手順

-
- ステップ 1** [スタート (Start)]>[すべてのプログラム (All Programs)]>[Cisco Unified CCE ツール (Cisco Unified CCE Tools)]>[ICMdba] を選択します。警告が表示されたら [はい (Yes)] をクリックします。
- ステップ 2** [サーバ (Server)]>[インスタンス (Instance)] に移動します。
- ステップ 3** インスタンス名を右クリックし、[作成 (Create)] を選択します。
- ステップ 4** [コンポーネントの選択 (Select Component)] 画面で、[管理 & データ サーバ (Administration & Data Server)] を選択します。
- ステップ 5** [AW タイプの選択 (Select AW Type)] ダイアログボックスで、[エンタープライズ (Enterprise)] を選択します。[OK] をクリックして、[データベースの作成 (Create Database)] ダイアログボックスを開きます。
- ステップ 6** データベースを作成し、次のようにログを作成します。
- [DB Type] フィールドで [AW] を選択します。
 - [ストレージ (Storage)] ペインで、[追加 (Add)] をクリックします。
 - [データ (Data)] をクリックします
 - C ドライブを選択します。
 - [サイズ (Size)] フィールドに 1400 MB と入力します。
 - [OK] をクリックして、[データベースの作成 (Create Database)] ダイアログボックスに戻ります。
 - [追加 (Add)] を再度クリックします。
 - [デバイスの追加 (Add Device)] ダイアログボックスで、[ログ (Log)] をクリックします。
 - C ドライブを選択します。
 - [サイズ (Size)] フィールドに 100 MB と入力します。
 - [OK] をクリックして、[データベースの作成 (Create Database)] ダイアログボックスに戻ります。
- ステップ 7** [データベースの作成 (Create Database)] ダイアログボックスで、[作成 (Create)] をクリックします。[開始 (Start)] をクリックします。作成の成功メッセージが表示されたら、[OK] と [閉じる (Close)] を順にクリックします。
-

管理サーバおよびリアルタイム データ サーバのコンポーネントの設定

手順

- ステップ 1** [Unified CCE Web セットアップ (Unified CCE Web Setup)]に進みます。
- ステップ 2** [コンポーネント管理 (Component Management)]>[管理サーバとデータ サーバ (Administration & Data Servers)]を選択します。[追加 (Add)]をクリックします。
- ステップ 3** [管理サーバとデータ サーバの追加 (Add Administration & Data Servers)]ページで、次のように設定します。
- 現在のインスタンスを選択します。
 - [エンタープライズ (Enterprise)]をクリックします。次に、[小規模から中規模の展開サイズ (Small to Medium Deployment Size)]をクリックします。
 - [次へ (Next)]をクリックします。
- ステップ 4** [Role]ページで、オプション[管理サーバおよびリアルタイム データ サーバ (AW) (Administration Server and Real-time Data Server (AW))]を選択します。[次へ (Next)]をクリックします。
- ステップ 5** A 側の [管理 & データ サーバの接続 (Administration & Data Servers Connectivity)]ページで、次の内容を実行します。
- [プライマリ管理 & データ サーバ (Primary Administration & Data Server)]のオプション ボタンをクリックします。
 - [プライマリ管理 & データ サーバ (*Primary Administration & Data Server)]フィールドに、A 側のサーバのホスト名を入力します。
 - [プライマリ/セカンダリ ペア (サイト) 名 (*Primary/Secondary Pair (Site) Name)]フィールドに AW_SideA を入力します。
 - [次へ (Next)]をクリックします。
- または、B 側の [管理 & データ サーバの接続 (Administration & Data Servers Connectivity)]ページで、次の内容を実行します。
- [プライマリ管理 & データ サーバ (Primary Administration & Data Server)]のオプション ボタンをクリックします。
 - [プライマリ管理 & データ サーバ (*Primary Administration & Data Server)]フィールドに、B 側のサーバのホスト名を入力します。
 - [プライマリ/セカンダリ ペア (サイト) 名 (*Primary/Secondary Pair (Site) Name)]フィールドに AW_SideB を入力します。
 - [次へ (Next)]をクリックします。
- ステップ 6** [データベースとオプション (Database and Options)]ページで、次のように設定します。
- [次のドライブ上でデータベースを作成 (Create Database(s) on Drive)]フィールドで、[C] を選択します。

- b) [エージェントのスキル変更 (Agent Re-skilling)] または [設定管理サービス (Configuration Management Service)] をクリックしないでください。
- c) [エージェントのスキル変更 (Agent Re-skilling)] Web ツールをクリックしないでください。
- d) [Internet Script Editor (ISE) Server] をオンにします。
- e) [次へ (Next)] をクリックします。

ステップ 7 [セントラル コントローラの接続 (Central Controller Connectivity)] ページで、次のように設定します。

- a) ルータ A 側には、コール サーバ A 側のパブリック ホスト名を入力します。
- b) ルータ B 側には、コール サーバ B 側のパブリック ホスト名を入力します。
- c) ロガー A 側には、データ サーバ A 側のパブリック ホスト名を入力します。
- d) ロガー B 側には、データ サーバ B 側のパブリック ホスト名を入力します。
- e) [セントラル コントローラ ドメイン名 (Central Controller Domain Name)] を入力します。
- f) どちらの側にいるかに応じて、[中央コントローラの A 側を優先 (Central Controller Side A Preferred)] または [中央コントローラの B 側を優先 (Central Controller Side B Preferred)] をクリックします。
- g) [次へ (Next)] をクリックします。

ステップ 8 [サマリー (Summary)] ページの内容を確認してから、[完了 (Finish)] をクリックします。

Unified Intelligence Center の SQL ユーザ アカウントの設定

手順

ステップ 1 [スタート (Start)] > [すべてのプログラム (All Programs)] > [Microsoft SQL Server 2008 R2] > [SQL Server Management Studio] に移動します。

ステップ 2 ログインします。

ステップ 3 [セキュリティ (Security)] > [ログイン (Logins)] に移動し、[ログイン (Logins)] を右クリックし、[新しいログイン (New Login)] を選択します。
このログインは、Cisco Unified Intelligence Center レポート用データ ソースを設定するときに使用されます。

ステップ 4 [全般 (General)] 画面で、次を実行します。

- a) ログイン名を入力します。
- b) [SQL Server 認証 (SQL Server authentication)] を選択します。
- c) パスワードを入力して確認します。
- d) [パスワード ポリシーを適用する (Enforce password policy)] をオフにします。

ステップ 5 [ユーザ マッピング (User Mapping)] をクリックします。

- a) A 側と AWdb に関連付けられているデータベースをオンにします。

- b) 各データベースを選択し、db_datareader ロールと public ロールに関連付けてから、[OK] をクリックします。
-



第 11 章

Cisco Unified CCE コール サーバ

この章には、A 側と B 側の Unified CCE コール サーバに対して実行する必要がある設定手順が含まれます。

- [Unified CCE ルータの設定, 128 ページ](#)
- [Generic PG の追加, 128 ページ](#)
- [PIM1 の追加 \(CUCM PIM\) , 129 ページ](#)
- [PIM2 の追加 \(最初の VRU PIM\) , 130 ページ](#)
- [PIM3 の追加 \(2 番目の VRU PIM\) , 131 ページ](#)
- [PIM4 の追加 \(3 番目の VRU PIM\) , 132 ページ](#)
- [PIM5 の追加 \(4 番目の VRU PIM\) , 133 ページ](#)
- [PIM の作成後, 133 ページ](#)
- [CTI サーバの設定, 135 ページ](#)
- [JTAPI のインストール, 136 ページ](#)
- [メディア ルーティング ペリフェラル ゲートウェイの設定, 136 ページ](#)
- [CTI OS サーバの設定, 138 ページ](#)

Unified CCE ルータの設定

手順

-
- ステップ 1 [Unified CCE Web セットアップ (Unified CCE Web Setup)] を起動します。
 - ステップ 2 ローカルの管理者権限を持つドメイン ユーザとしてサインインします。
 - ステップ 3 [インスタンス管理 (Instance Management)] をクリックし、[追加 (Add)] をクリックします。
 - ステップ 4 [インスタンスの追加 (Add Instance)] ダイアログボックスで、お客様のファシリティとインスタンスを選択します。
 - ステップ 5 [インスタンス番号 (Instance Number)] フィールドに 0 と入力します。[保存 (Save)] をクリックします。
 - ステップ 6 [コンポーネント管理 (Component Management)] > [ルータ (Routers)] を選択します。
 - ステップ 7 [追加 (Add)] をクリックして Call Router をセットアップします。
 - ステップ 8 [展開 (Deployment)] ページで、該当する側をクリックします。
 - ステップ 9 [デュプレックス (Duplexed)] をクリックします。[次へ (Next)] をクリックします。
 - ステップ 10 [ルータ接続 (Router Connectivity)] ページで、プライベートインターフェイスとパブリック (表示) インターフェイスを設定します。[次へ (Next)] をクリックします。
 - ステップ 11 [Peripheral Gateway の有効化 (Enable Peripheral Gateways)] ページで、[Peripheral Gateway を有効にする (Enable Peripheral Gateways)] フィールドに 1-2 と入力します。[次へ (Next)] をクリックします。
 - ステップ 12 [ルータ オプション (Router Options)] ページで、[Quality of Service (QoS) を有効にする (Enable Quality of Service (QoS))] チェックボックスをオンにし、[次へ (Next)] をクリックします。
(注) この手順は、A 側のみに適用します。
 - ステップ 13 [ルータ QoS (Router Quality of Service)] ウィンドウで、[次へ (Next)] をクリックします。
 - ステップ 14 [サマリー (Summary)] ページで、ルータ サマリーが正しいことを確認し、[完了 (Finish)] をクリックします。
-

Generic PG の追加

Generic PG は、最初に追加する PG である必要があります。PG1 の PG ID が割り当てられます。

手順

-
- ステップ 1** [スタート (Start)] > [すべてのプログラム (All Programs)] > [Cisco Unified CCE ツール (Cisco Unified CCE Tools)] > [Peripheral Gateway のセットアップ (Peripheral Gateway Setup)] を選択します。
- ステップ 2** [インスタンス コンポーネント (Instance Components)] ペインで [追加 (Add)] をクリックし、[コンポーネントの選択 (Component Selection)] ダイアログボックスから [Peripheral Gateway] を選択します。
- ステップ 3** [Peripheral Gateway プロパティ (Peripheral Gateway Properties)] ダイアログボックスで、次を実行します。
- [実稼働モード (Production mode)] をオンにします。
 - [システムの起動時に自動的に起動する (Auto start system startup)] をオンにします。
 - [デュプレックス Peripheral Gateway (Duplexed Peripheral Gateway)] をオンにします。
 - [PG ノードのプロパティ ID (PG node Properties ID)] フィールドで、[PG1] を選択します。
 - 適切な側 ([A 側 (Side A)] または [B 側 (Side B)]) を選択します。
 - [クライアント タイプ (Client Type)] ペインで、選択したタイプに [CUCM] および [VRU] を追加します。
 - [次へ (Next)] をクリックします。
-

PIM1 の追加 (CUCM PIM)

手順

-
- ステップ 1** [Peripheral Gateway コンポーネント プロパティ (Peripheral Gateway Component Properties)] ダイアログボックスの [ペリフェラル インターフェイス マネージャ (Peripheral Interface Manager)] ペインで、[追加 (Add)] をクリックします。
- ステップ 2** [CUCM] および [PIM1] を選択します。 [OK] をクリックします。
- ステップ 3** [有効 (Enabled)] をオンにします。
- ステップ 4** [Peripheral 名 (Peripheral name)] フィールドに CM と入力します。
- ステップ 5** [Peripheral ID] フィールドに 5000 と入力します。
- ステップ 6** [エージェントの内線番号長 (Agent extension length)] フィールドに、この展開の内線番号の長さを入力します。
- ステップ 7** [Unified Communications Manager パラメータ (Unified Communications Manager Parameters)] ペインで、次のように設定します。
- [サービス (Service)] フィールドに、Unified Communications Manager サブスクリバのホスト名を入力します。
 - [ユーザ ID (User ID)] フィールドに pguser と入力します。

- c) [ユーザ パスワード (User Password)] フィールドに、Unified Communications Manager に作成するユーザのパスワードを入力します。
- d) [Mobile Agent Codec] フィールドで、[G711 ULAW/ALAW] または [G.729] を選択します。

ステップ 8 [OK] をクリックします。

PIM2 の追加 (最初の VRU PIM)

手順

- ステップ 1** [Peripheral Gateway コンポーネント プロパティ (Peripheral Gateway Component Properties)] ダイアログボックスの [ペリフェラル インターフェイス マネージャ (Peripheral Interface Manager)] ページで、[追加 (Add)] をクリックします。
 - ステップ 2** [VRU のクライアント タイプ (Client Type of VRU)] および [PIM2] を選択します。[OK] をクリックします。
 - ステップ 3** [有効 (Enabled)] をオンにします。
 - ステップ 4** [Peripheral 名 (Peripheral name)] フィールドに CVP1 と入力します。
 - ステップ 5** [Peripheral ID] フィールドに 5001 と入力します。
 - ステップ 6** [VRU ホスト名 (VRU hostname)] フィールドに CVP1 (A 側) のホスト名を入力します。
 - ステップ 7** [VRU 接続ポート (VRU Connect port)] フィールドに、5000 と入力します。
 - ステップ 8** [再接続間隔 (秒) (Reconnect interval (sec))] フィールドに、10 と入力します。
 - ステップ 9** [ハートビート間隔 (秒) (Heartbeat interval (sec))] フィールドに、5 と入力します。
 - ステップ 10** [DSCP] フィールドで [CS3(24)] を選択します。
 - ステップ 11** [OK] をクリックします。
-

PIM3 の追加 (2 番目の VRU PIM)

手順

-
- ステップ 1 [Peripheral Gateway コンポーネント プロパティ (Peripheral Gateway Component Properties)] ダイアログボックスの [ペリフェラル インターフェイス マネージャ (Peripheral Interface Manager)] ペインで、[追加 (Add)] をクリックします。
 - ステップ 2 [VRU のクライアント タイプ (Client Type of VRU)] および [PIM3] を選択します。 [OK] をクリックします。
 - ステップ 3 [有効 (Enabled)] をオンにします。
 - ステップ 4 [Peripheral 名 (Peripheral name)] フィールドに CVP2 と入力します。
 - ステップ 5 [Peripheral ID] フィールドに 5002 と入力します。
 - ステップ 6 VRU ホスト名に CVP1 (B 側) の IP アドレスを入力します。
 - ステップ 7 [VRU 接続ポート (VRU Connect port)] フィールドに、5000 と入力します。
 - ステップ 8 [再接続間隔 (秒) (Reconnect interval (sec))] フィールドに、10 と入力します。
 - ステップ 9 [ハートビート間隔 (秒) (Heartbeat interval (sec))] フィールドに、5 と入力します。
 - ステップ 10 [DSCP] フィールドで [CS3(24)] を選択します。
 - ステップ 11 [OK] をクリックします。
-

PIM4 の追加 (3 番目の VRU PIM)

手順

-
- ステップ 1 [Peripheral Gateway コンポーネントプロパティ (Peripheral Gateway Component Properties)] ダイアログボックスの [ペリフェラルインターフェイス マネージャ (Peripheral Interface Manager)] ペインで、[追加 (Add)] をクリックします。
 - ステップ 2 [VRU のクライアントタイプ (Client Type of VRU)] および [PIM4] を選択します。 [OK] をクリックします。
 - ステップ 3 [有効 (Enabled)] をオンにします。
 - ステップ 4 [Peripheral 名 (Peripheral name)] フィールドに CVP3 と入力します。
 - ステップ 5 [Peripheral ID] フィールドに 5003 と入力します。
 - ステップ 6 VRU ホスト名に CVP2 (A 側) の IP アドレスを入力します。
 - ステップ 7 [VRU 接続ポート (VRU Connect port)] フィールドに、5000 と入力します。
 - ステップ 8 [再接続間隔 (秒) (Reconnect interval (sec))] フィールドに、10 と入力します。
 - ステップ 9 [ハートビート間隔 (秒) (Heartbeat interval (sec))] フィールドに、5 と入力します。
 - ステップ 10 [DSCP] フィールドで [CS3(24)] を選択します。
 - ステップ 11 [OK] をクリックします。
-

PIM5 の追加 (4 番目の VRU PIM)

手順

-
- ステップ 1** [Peripheral Gateway コンポーネント プロパティ (Peripheral Gateway Component Properties)] ダイアログボックスの [ペリフェラル インターフェイス マネージャ (Peripheral Interface Manager)] ペインで、[追加 (Add)] をクリックします。
- ステップ 2** [VRU のクライアント タイプ (Client Type of VRU)] および [PIM4] を選択します。[OK] をクリックします。
- ステップ 3** [有効 (Enabled)] をオンにします。
- ステップ 4** [Peripheral 名 (Peripheral name)] フィールドに CVP4 と入力します。
- ステップ 5** [Peripheral ID] フィールドに 5004 と入力します。
- ステップ 6** VRU ホスト名に CVP2 (B 側) の IP アドレスを入力します。
- ステップ 7** [VRU 接続ポート (VRU Connect port)] フィールドに、5000 と入力します。
- ステップ 8** [Reconnect interval (sec)] フィールドに、10 と入力します。
- ステップ 9** [Heartbeat interval (sec)] フィールドに、5 と入力します。
- ステップ 10** [DSCP] フィールドで [CS3(24)] を選択します。
- ステップ 11** [OK] をクリックします。
-

PIM の作成後

[Peripheral Gateway Component Properties] ページでこのタスクを実行します。

手順

-
- ステップ 1** [論理コントローラ ID (Logical Controller ID)] フィールドに 5000 と入力します。
- ステップ 2** [CTI コール後処理データ遅延 (CTI Call Wrapup Data delay)] フィールドに 0 と入力します。
- ステップ 3** [VRU レポート (VRU Reporting)] ペインで、[サービス制御 (Service Control)] をクリックし、[キュー レポート (Queue Reporting)] をオンにします。[次へ (Next)] をクリックして [デバイス管理プロトコルのプロパティ (Device Management Protocol Properties)] ダイアログボックスを開きます。
- ステップ 4** [Device Management Protocols Properties] ダイアログボックスで、すべてのインターフェイス フィールドに値を入力します。
- a) A 側 PG の場合 :
- [Side A Preferred] を選択します。

- [Side A Properties] で、[Call Router is local] をオンにします。
- [Side B Properties] で、[Call Router is remote (WAN)] をオンにします。

b) B 側 PG の場合 :

- [Side B Preferred] を選択します。
- [Side A Properties] で、[Call Router is remote (WAN)] をオンにします。
- [Side B Properties] で、[Call Router is local] をオンにします。

c) 両方の場合 :

- [使用可能な帯域幅 (kbps) (Usable Bandwidth (kbps))] フィールドで、デフォルトの値を受け入れます。
- [ハートビート間隔 (100 ミリ秒) (Heartbeat Interval (100ms))] フィールドで、デフォルトの値を受け入れます。

d) [次へ (Next)] をクリックします。

ステップ 5 [Peripheral Gateway ネットワーク インターフェイス (Peripheral Gateway Network Interfaces)] ダイアログボックスで、すべてのインターフェイス フィールドに値を入力します。

- a) プライベートと可表示のネットワーク インターフェイスのホスト名を入力します。PG とルータ エントリの場合、プライベートとプライベートハイに同じホスト名を使用し、可表示と可表示ハイに同じホスト名を使用します。
- b) A 側のプライベート インターフェイスのセクション内にある [QoS] ボタンをクリックします。[PG プライベート リンク QoS 設定 (PG Private Link QoS Settings)] で、[QoS を有効にする (Enable QoS)] をオンにし、[OK] をクリックします。
- c) A 側と B 側の両方の PG の可表示インターフェイスのセクション内にある [QoS] ボタンをクリックします。[PG 表示リンク QoS 設定 (PG Visible Link QoS Settings)] で、[QoS を有効にする (Enable QoS)] をオンにし、[OK] をクリックします。
- d) [次へ (Next)] をクリックします。

ステップ 6 [セットアップ情報の確認 (Check Setup Information)] ダイアログボックスで、[次へ (Next)] をクリックします。

ステップ 7 [セットアップの完了 (Setup Complete)] ダイアログボックスで、[完了 (Finish)] をクリックします。

CTI サーバの設定

手順

-
- ステップ 1** [Start] > [All Programs] > [Cisco Unified CCE Tools] > [Peripheral Gateway Setup] を選択します。
- ステップ 2** [コンポーネントのセットアップ (Components Setup)] ダイアログボックスの [インスタンス コンポーネント (Instance Components)] ペインで、[追加 (Add)] をクリックします。
- ステップ 3** [コンポーネントの選択 (Component Selection)] ダイアログボックスで [CTI サーバ (CTI Server)] をクリックします。
- a) [実稼働モード (Production mode)] をオンにします。
 - b) [システムの起動時に自動的に起動する (Auto start at system startup)] をオンにします。
 - c) [デュプレックス CTI サーバ (Duplexed CTI Server)] をオンにします。
 - d) [CG ノードのプロパティ (CG node properties)] ペインの [ID] フィールドで、[CG1] を選択します。
 - e) [CG ノードのプロパティ (CG node properties)] の [ICM システム ID (ICM system ID)] フィールドに 1 と入力します。
 - f) 適切な側をクリックします。
 - g) [次へ (Next)] をクリックします。
- ステップ 4** [サーバコンポーネントのプロパティ (Server Component Properties)] ダイアログボックスで、次のように設定します。
- a) A 側については、[クライアント接続ポート番号 (Client Connection Port Number)] フィールドに 42027 と入力します。
 - b) B 側については、[クライアント接続ポート番号 (Client Connection Port Number)] フィールドに 43027 と入力します。
- ステップ 5** [次へ (Next)] をクリックします。
- ステップ 6** [ネットワーク インターフェイスのプロパティ (Network Interface Properties)] ダイアログボックスでは、すべてのインターフェイス フィールドを入力し、[次へ (Next)] をクリックします。
- ステップ 7** [セットアップ情報の確認 (Check Setup Information)] ページで、[次へ (Next)] をクリックします。
- ステップ 8** [セットアップ完了 (Setup Completed)] ダイアログボックスで、[完了 (Finish)] をクリックします。
- ステップ 9** [セットアップを終了する (Exit Setup)] をクリックします。
-

JTAPI のインストール

手順

-
- ステップ 1** Unified CCE コール サーバのブラウザで Unified Communications Manager を起動し (https://{callmanager-hostname/ccmadmin})、サインインします。
- ステップ 2** [アプリケーション (Application)] > [プラグイン (Plugins)] に移動します。[検索 (Find)] をクリックします。
- ステップ 3** Windows 対応の Cisco JTAPI 32-bit Client をダウンロードします。
- ステップ 4** ダウンロードしたファイルをインストールし、すべてのデフォルト設定を受け入れます。
- ステップ 5** プロンプトで、Unified Communications Manager TFTP サーバの IP アドレスを入力します。
- ステップ 6** [終了 (Finish)] をクリックします。
-

メディアルーティングペリフェラルゲートウェイの設定

CCEメディアルーティングペリフェラルゲートウェイを設定するには、次の手順を実行します。メディアルーティングペリフェラルゲートウェイは必須です。これを設定する必要があります。MR PG 用の PIM の作成は任意です。必要に応じて、最大 4 つの PIM を作成できます。メディアルーティングペリフェラルゲートウェイには、次の 4 つの PIM を任意に設定できます。

- 送信 PIM
- SocialMiner に対するマルチチャネル PIM
- E-Mail and Web Interaction Manager に対するマルチチャネル PIM
- サードパーティのマルチチャネルアプリケーションに対するマルチチャネル PIM

ペリフェラルゲートウェイの設定を使用して PIM を作成し、システムの導入ツールを使用して外部マシンを追加するまでは、マルチチャネル PIM に関連付けられたダイヤル番号を作成できません。



-
- (注) アウトバウンド PIM およびマルチチャネル PIM の追加の手順については、URL http://www.cisco.com/en/US/products/ps12586/prod_maintenance_guides_list.html の機能ガイドを参照してください。
-

メディアルーティング PG の追加

MR PG は、PG2 の PG ID が割り当てられるようにユーザが追加する 2 番目の PG である必要があります。A 側では PG2A です。B 側では PG2B です。

手順

-
- ステップ 1** [スタート (Start)]>[プログラム (Programs)]>[Cisco Unified CCE ツール (Cisco Unified CCE Tools)]>[Peripheral Gateway セットアップ (Peripheral Gateway Setup)] を選択します。
- ステップ 2** [インスタンス コンポーネント (Instance Components)] ペインで [追加 (Add)] をクリックし、[コンポーネントの選択 (Component Selection)] ダイアログボックスから [Peripheral Gateway] を選択します。
- ステップ 3** [Peripheral Gateway プロパティ (Peripheral Gateway Properties)] ダイアログボックスで、次を実行します。
- [実稼働モード (Production Mode)] をオンにします。
 - [システムの起動時に自動的に起動する (Auto start system startup)] をオンにします。
 - [デュプレックス Peripheral Gateway (Duplexed Peripheral Gateway)] をオンにします。
 - [PG ノード プロパティ ID (PG node Properties ID)] フィールドで [PG2] を選択します。
 - 適切な側をクリックします。
 - [クライアント タイプ (Client Type)] ペインで、選択したタイプに [メディアルーティング (Media Routing)] を追加します。
 - [次へ (Next)] をクリックします。
- ステップ 4** [論理コントローラ ID (Logical Controller ID)] フィールドに 5001 と入力します。
- ステップ 5** [CTI コール後処理データ遅延 (CTI Call Wrapup Data delay)] フィールドに 0 と入力します。[次へ (Next)] をクリックします。
- ステップ 6** [デバイス管理プロトコルのプロパティ (Device Management Protocol Properties)] ダイアログボックスで、次のように設定します。
- A 側 PG の場合 :
 - [Side A Preferred] を選択します。
 - [Side A Properties] で、[Call Router is local] をオンにします。
 - [Side B Properties] で、[Call Router is remote (WAN)] をオンにします。
 - B 側 PG の場合 :
 - [Side B Preferred] を選択します。
 - [Side A Properties] で、[Call Router is remote (WAN)] をオンにします。
 - [Side B Properties] で、[Call Router is local] をオンにします。
 - 両方の場合 :

- [使用可能な帯域幅 (kbps) (Usable Bandwidth (kbps))] フィールドで、デフォルトの値を受け入れます。
- [ハートビート間隔 (100 ms) (Heartbeat Interval (100ms))] フィールドに **4** と入力します。

d) [次へ (Next)] をクリックします。

ステップ 7 [Peripheral Gateway ネットワーク インターフェイス (Peripheral Gateway Network Interfaces)] ダイアログボックスで、プライベート インターフェイスと表示インターフェイスを入力します。

- a) プライベートと可表示のネットワーク インターフェイスのホスト名を入力します。PG とルータ エントリの場合、プライベートとプライベート ハイに同じホスト名を使用し、可表示と可表示ハイに同じホスト名を使用します。
- b) A 側のプライベート インターフェイスのセクション内にある [QoS] ボタンをクリックします。[PG Private Link QoS Settings] で、[Enable QoS] をオンにし、[OK] をクリックします。
- c) A 側と B 側の両方の PG の可表示インターフェイスのセクション内にある [QoS] ボタンをクリックします。[PG Visible Link QoS Settings] で、[Enable QoS] をオンにし、[OK] をクリックします。
- d) [次へ (Next)] をクリックします。

ステップ 8 [セットアップ情報の確認 (Check Setup Information)] ダイアログボックスで、[次へ (Next)] をクリックします。

ステップ 9 [セットアップの完了 (Setup Complete)] ダイアログボックスで、[完了 (Finish)] をクリックします。

ステップ 10 [セットアップを終了する (Exit Setup)] をクリックします。

CTI OS サーバの設定



(注) お客様がエージェント デスクトップに対して Finesse を使用する場合、この手順は必要ありません。

手順

- ステップ 1** Unified CCE コールサーバのローカル ドライブに CTIOS ISO イメージをマウントするか、CTIOS インストーラをコピーします。
- ステップ 2** CTIOS のメンテナンス リリースが提供されている場合は、そのメンテナンス リリースを Unified CCE コールサーバのローカル ドライブにコピーします。
- ステップ 3** CTIOS Server に移動し、`setup.exe` を実行します。SNMP サービスが停止され、インストールの完了後に再び起動されることを示す警告に対して [はい (Yes)] をクリックします。
- ステップ 4** ソフトウェア使用許諾契約に同意します。
- ステップ 5** 最新のメンテナンス リリースがある場合は、その場所を参照します。[次へ (Next)] をクリックします。
- ステップ 6** [CTIOS インスタンス (CTI OS Instance)] ダイアログボックスで、[CTIOS インスタンス リスト (CTI OS Instance List)] ペインをクリックします。[CTIOS サーバ インスタンスの追加 (Add CTIOS Server Instance)] ウィンドウでは、インスタンス名を入力し、[OK] をクリックします。
- ステップ 7** [CTIOS サーバリスト (CTI OS Server List)] ペインで、[追加 (Add)] をクリックします。[OK] をクリックします。
- ステップ 8** [デスクトップ ドライブの入力 (Enter Desktop Drive)] ダイアログボックスで、ドライブ C を選択します。[OK] をクリックします。
- ステップ 9** [CTI サーバ名 (CTI Server Information)] ダイアログボックスでは、コールサーバのホスト名、A 側のポート (42027) 、および B 側のポート (43027) を入力します。次に、[次へ (Next)] をクリックします。
- ステップ 10** [Peripheral ID (Peripheral Identifier)] ダイアログボックスで、すべてのデフォルトを受け入れ、[次へ (Next)] をクリックします。
- ステップ 11** [接続情報 (Connect Information)] ダイアログボックスで、すべてのデフォルトを受け入れ、[次へ (Next)] をクリックします。
- ステップ 12** [統計情報 (Statistics Information)] ダイアログボックスで、デフォルトを受け入れ、[次へ (Next)] をクリックします。
- ステップ 13** [IPCC サイレント モニタ タイプ (IPCC Silent Monitor Type)] ダイアログボックスで、[サイレント モニタ タイプ (Silent Monitor Type)] を [CCM ベース (CCM Based)] に設定し、[次へ (Next)] をクリックします。
- ステップ 14** [ピア CTIOS サーバ (Peer CTIOS Server)] ダイアログボックスで、次のように設定します。
- a) [デュプレックス CTIOS インストール (Duplex CTIOS Install)] をオンにします。
 - b) A 側を設定している場合、ピア CTIOS サーバをコールサーバの A 側のホスト名に設定します。B 側を設定している場合、ピア CTIOS サーバをコールサーバの B 側のホスト名に設定します。

c) [ポート (Port)]フィールドに、**42028** と入力します。

ステップ 15 [終了 (Finish)]をクリックします。

ステップ 16 [Cisco CTIOS サーバセキュリティ (Cisco CTIOS Server Security)]ダイアログボックスで、[セキュリティを有効にする (Enable Security)]をオフにします。[OK]をクリックします。

ステップ 17 [CTIOS セキュリティセットアップの完了 (CTIOS Security Setup Complete)]ダイアログボックスで、[完了 (Finish)]をクリックします。

ステップ 18 コンピュータを再起動することを要求するプロンプトが表示されたら、[はい (Yes)]をクリックします。メンテナンスリリースが存在する場合は、そのインストールが自動的に開始されます。

ステップ 19 メンテナンス リリースが存在する場合は、すべての指示に従ってメンテナンス リリースをインストールします。

ステップ 20 メンテナンスリリースのインストールが完了したら、[完了 (Finish)]をクリックし、指示に従って再起動します。

ステップ 21 レジストリエディタにアクセスします ([スタート (Start)]>[ファイル名を指定して実行 (Run)]> **regedit**) 。

ステップ 22 [**HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems,Inc.\Ctios\CTIOS_
instance name>\CTIOS1\Server\Agent**] に移動します。

ステップ 23 [forceLogoutOnSessionClose] を **1** に設定します。



第 12 章

Cisco Unified Customer Voice Portal

この章では、A 側と B 側に Cisco Unified CVP コールおよび OAMP サーバを設定するために実行する必要がある手順について説明します。

- [ネットワーク カードの検証, 142 ページ](#)
- [Unified CVP コール サーバの設定, 142 ページ](#)
- [Unified CVP VXML サーバの設定, 143 ページ](#)
- [ゲートウェイの設定, 144 ページ](#)
- [Unified CVP Media Server の設定, 144 ページ](#)
- [スクリプトおよびメディア ファイルの転送, 145 ページ](#)
- [ライセンス ファイルの転送, 145 ページ](#)
- [SNMP の設定, 146 ページ](#)
- [SIP サーバグループの設定, 146 ページ](#)
- [ダイヤル番号パターンの設定, 147 ページ](#)
- [Location-Based コール アドミッション制御, 149 ページ](#)

ネットワークカードの検証

手順

-
- ステップ 1 [スタート (Start)] を選択し、[ネットワーク (Network)] を右クリックします。
 - ステップ 2 [プロパティ (Properties)] を選択します。次に、[アダプタの設定の変更 (Change Adapter Settings)] を選択します。
 - ステップ 3 [ローカルエリア接続 (Local Area Connection)] を右クリックして、[プロパティ (Properties)] を選択します。
 - ステップ 4 [インターネットプロトコルバージョン 6 (TCP/IPv6) (Internet Protocol Version 6 (TCP/IPv6))] をオフにします。
 - ステップ 5 [インターネットプロトコルバージョン 4 (Internet Protocol Version 4)] をオンにして、[プロパティ (Properties)] を選択します。
 - ステップ 6 テンプレートのビジブル IP アドレス、サブネットマスク、デフォルトゲートウェイ、および優先 DNS サーバおよび代替 DNS サーバのデータを確認します。
 - ステップ 7 [OK] をクリックします。
-

Unified CVP コールサーバの設定

Unified CVP サーバ上でコールサーバコンポーネントを設定するには、次の手順を実行します。

手順

-
- ステップ 1 Unified CVPOAMP サーバで、[スタート (Start)] > [すべてのプログラム (All Programs)] > [Cisco Unified Customer Voice Portal] に進みます。
 - ステップ 2 [Operations Console] をクリックして、ログインします。
 - ステップ 3 [デバイス管理 (Device Management)] > [Unified CVP Call Server] に移動します。
 - ステップ 4 [新規追加 (Add New)] をクリックします。
 - ステップ 5 [一般 (General)] タブで、Cisco Unified CVP サーバの IP アドレスとホスト名を入力します。[ICM]、[IVR]、および [SIP] をオンにします。[次へ (Next)] をクリックします。
 - ステップ 6 [SIP] タブをクリックします。
 - a) [アウトバウンドプロキシを有効にする (Enable outbound proxy)] フィールドで、[いいえ (No)] を選択します。
 - b) [DNS SRV タイプクエリーの使用 (Use DNS SRV type query)] フィールドで、[はい (Yes)] を選択します。

c) [SRV レコードをローカルに解決 (Resolve SRV records locally)] をオンにします。

ステップ 7 (任意) [インフラストラクチャ (Infrastructure)] タブをクリックします。[Syslog 設定 (Configuration Syslog Settings)] ペインで、次のようにフィールドを設定します。

- a) syslog サーバの IP アドレスまたはホスト名を入力します。
- b) syslog サーバのポート番号として **514** を入力します。
- c) レポートングサーバがログメッセージを書き込むバックアップサーバの名前を入力します。
- d) [バックアップ サーバ ポート番号 (Backup server port number)] フィールドに、バックアップ syslog サーバのポート番号を入力します。

ステップ 8 [保存して展開 (Save & Deploy)] をクリックします。

ステップ 9 次の 3 つの Unified CVP サーバについて、この手順を繰り返します。

Unified CVP VXML サーバの設定

Cisco Unified CVP サーバ上で VXML サーバ コンポーネントを設定するには、次の手順を実行します。

手順

ステップ 1 Unified CVP Operations Console で、[デバイス管理 (Device Management)] > [Unified CVP VXML Server] に移動します。

ステップ 2 [新規追加 (Add New)] をクリックします。

ステップ 3 [一般 (General)] タブで、Cisco Unified CVP サーバの IP アドレスとホスト名を入力します。

ステップ 4 プライマリとバックアップの CVP コールサーバを次のように設定します。

- a) CVP-1A の場合、プライマリ コールサーバは CVP-1A、バックアップ コールサーバは CVP-1B です。
- b) CVP-2A の場合、プライマリ コールサーバは CVP-2A、バックアップ コールサーバは CVP-2B です。
- c) CVP-1B の場合、プライマリ コールサーバは CVP-1B、バックアップ コールサーバは CVP-1A です。
- d) CVP-2B の場合、プライマリ コールサーバは CVP-2B、バックアップ コールサーバは CVP-2A です。

ステップ 5 [保存して展開 (Save & Deploy)] をクリックします。

ステップ 6 すべての CVP サーバについて、この手順を繰り返します。

ゲートウェイの設定

手順

-
- ステップ 1** Unified CVP Operations Console で、[デバイス管理 (Device Management)] > [ゲートウェイ (Gateway)] に移動します。
- ステップ 2** [新規追加 (Add New)] をクリックします。
- ステップ 3** [一般 (General)] タブで、次のように設定します。
- IP アドレスを入力します。
 - ホスト名を入力します。
 - デバイス タイプを選択します。
 - [ユーザ名とパスワード (Username and Password)] ペインに、ユーザ名とパスワードを入力し、パスワードを有効にします。
- ステップ 4** [保存 (Save)] をクリックします。
- ステップ 5** すべてのゲートウェイに対して繰り返し行ってください。
-

Unified CVP Media Server の設定

手順

-
- ステップ 1** Unified CVP Operations Console で、[デバイス管理 (Device Management)] > [メディアサーバ (Media Server)] に移動します。
- ステップ 2** [新規追加 (Add New)] をクリックします。
- ステップ 3** [General] タブで、次の項目を設定します。
- Unified CVP サーバの IP アドレスとホスト名を入力します。
 - [FTP Enabled] をオンにします。
 - [Anonymous Access] をオンにするか、資格情報を入力します。
 - [Test SignIn] をクリックして、FTP アクセスを検証します。
- ステップ 4** [保存 (Save)] をクリックします。
- ステップ 5** すべての CVP サーバに対してステップ 1 ~ 4 を繰り返します。
- ステップ 6** [デフォルト メディア サーバ (Default Media Server)] を [なし (None)] からいずれかの Unified CVP サーバに変更します。[設定 (Set)] をクリックします。
- ステップ 7** [展開 (Deploy)] をクリックします。
-

スクリプトおよびメディア ファイルの転送

通知先を作成し、すべての Unified CVP デバイスに展開します。

手順

-
- ステップ 1 Unified CVP Operations Console で、[一括管理 (Bulk Administration)] > [ファイル転送 (File Transfer)] > [スクリプト & メディア (Scripts & Media)] に移動します。
 - ステップ 2 [デバイス タイプの選択 (Select device type)] フィールドで、[ゲートウェイ (Gateway)] を選択します。
 - ステップ 3 すべてのゲートウェイを [選択済み (Selected)] に移動します。
 - ステップ 4 [デフォルト ゲートウェイ (Default Gateway)] のファイルをクリックします。
 - ステップ 5 [転送 (Transfer)] をクリックし、ポップアップ ウィンドウで [OK] を選択します。
 - ステップ 6 [ファイル転送ステータス (File Transfer Status)] をクリックして転送の進捗状況をモニタします。
-

ライセンス ファイルの転送

手順

-
- ステップ 1 Unified CVP Operations Console で、[一括管理 (Bulk Administration)] > [ファイル転送 (File Transfer)] > [ライセンス (Licenses)] に移動します。
 - ステップ 2 [参照 (Browse)] をクリックして、アップロードするライセンス ファイルを選択します。
 - ステップ 3 [転送 (Transfer)] をクリックします。次に、確認のメッセージで [OK] をクリックします。
 - ステップ 4 [ファイル転送ステータス (File Transfer Status)] をクリックします。
 - ステップ 5 各ファイル転送の [ステータス (Status)] 列に [成功 (Success)] と表示されていることを確認します。
 - ステップ 6 [システム (System)] > [コントロールセンター (Control Center)] に移動します。
 - ステップ 7 正常にシャットダウンしてから、リストの各コール サーバを起動します。これによって、新しいライセンスが有効になります。
-

SNMP の設定



(注) この手順は任意です。詳細については、[簡易ネットワーク管理プロトコル](#)、(229 ページ) を参照してください。

手順

-
- ステップ 1** Unified CVP Operations Console で、[SNMP] > [V1/V2c] > [コミュニティ スtring (Community String)] に移動します。
- ステップ 2** [新規追加 (Add New)] をクリックします。
- コミュニティ スtring に名前を付けます。
 - [デバイス (Devices)] タブを選択し、SNMP コミュニティ スtring をデバイスに割り当てます。
 - [保存して展開 (Save and Deploy)] をクリックします。
- ステップ 3** 通知先を作成し、すべての Unified CVP デバイスに展開します。
- [SNMP] > [V1/V2c] > [通知の送信先 (Notification Destination)] に移動します。
 - フィールドに入力します。
 - [デバイス (Devices)] タブを選択し、SNMP 通知先をデバイスに割り当てます。
 - [保存して展開 (Save and Deploy)] をクリックします。
-

SIP サーバグループの設定

SIP サーバグループは、Cisco Unified Communications Manager およびゲートウェイで必要となります。

手順

-
- ステップ 1** Unified CVP Operations Console で、[システム (System)] > [SIP サーバグループ (SIP Server Group)] に移動します。
- ステップ 2** Cisco Unified Communications Manager デバイス用のサーバグループを作成します。
- [一般 (General)] タブで、[新規追加 (Add New)] をクリックします。
 - [SRV ドメイン名 FQDN (SRV Domain Name FQDN)] フィールドに、Communications Manager のエンタープライズパラメータの Cluster FQDN 設定でも使用される値を入力します。たとえば、`cucm.cisco.com` のようになります。

- c) [IP アドレス/ホスト名 (IP Address/Hostname)]フィールドに、Unified Communications Manager ノードの IP アドレスまたはホスト名を入力します。
- d) [追加 (Add)]をクリックします。
- e) Unified Communications Manager サブスクリバごとにステップ c と d を繰り返します。[保存 (Save)]をクリックします。
(注) サーバグループにパブリッシャ ノードを挿入しないでください。

Communications Manager から SCC モデルの CVP に作成された直接 SIP トランクがないので、SCC の展開には Communications Manager の SIP サーバグループは必要ありません。

FQDN は、Cisco Unified Communications Manager のエンタープライズパラメータに設定される Cluster FQDN 設定に設定された FQDN に一致する必要があります。[完全修飾ドメイン名の設定 \(160 ページ\)](#) を参照してください。

ステップ 3 ゲートウェイ デバイス用にサーバグループを作成します。

- a) [一般 (General)]タブで、[新規追加 (Add New)]をクリックします。
- b) [SRV ドメイン名 SQRN (SRV Domain Name FQDN)]フィールドに、SRV ドメイン名の FQDN を入力します。たとえば、vxmlgw.cisco.com のようになります。
- c) [IP アドレス/ホスト名 (IP Address/Hostname)]フィールドに、各ゲートウェイの IP アドレスまたはホスト名を入力します。
- d) [追加 (Add)]をクリックします。
- e) ゲートウェイに対してステップ c と d を繰り返します。[保存 (Save)]をクリックします。展開と分岐に応じてすべての VXML ゲートウェイを追加します。すべての VXML ゲートウェイをサーバグループに追加すると、すべてのメンバサーバグループ ゲートウェイに対してコールのロード バランスが行われます。

ステップ 4 これらのサーバグループをすべての Unified CVP コール サーバに関連付けます。

- a) [コール サーバの展開 (Call Server Deployment)]タブで、すべての Unified CVP コール サーバを [使用可能 (Available)]リストから [選択済み (Selected)]リストに移動します。
- b) [保存して展開 (Save and Deploy)]をクリックします。

ダイヤル番号パターンの設定

ダイヤル番号パターンは、次の場合に必要です。

- エージェント デバイス
- ネットワーク VRU
- 呼出音
- エラー

手順

- ステップ 1** Unified CVP Operations Console で、[システム (System)]>[ダイヤル番号パターン (Dialed Number Pattern)]に移動します。
- ステップ 2** 次の表のダイヤル番号パターンごとに、次の手順を実行します。
- [新規追加 (Add New)]をクリックします。
 - [ダイヤル番号パターン (Dialed Number Pattern)]フィールドに、ダイヤル番号パターンを入力します。
 - [説明 (Description)]フィールドに、ダイヤル番号パターンの説明を入力します。
 - [ダイヤル番号パターンのタイプ (Dialed Number Pattern Types)]ペインで、指定したダイヤル番号パターンのタイプを確認します。
 - [保存 (Save)]をクリックします。
- ステップ 3** すべてのダイヤル番号パターンを設定した後、[展開 (Deploy)]をクリックします。
- ステップ 4** [展開ステータス (Deployment Status)]をクリックして、設定が適用されていることを確認します。

ダイヤル番号パターン	説明	ダイヤル番号パターンのタイプ
91*	呼出音	[ローカルスタティックルートを有効にする (Enable Local Static Route)]をオンにします。 SIP サーバグループ、および IP アドレス/ホスト名/サーバグループ名へのルートは、いずれも VXML ゲートウェイです (たとえば、vxmlgw.cisco.com) 。 [発信元へのコールの送信を有効にする (Enable Send Calls to Originator)]をオンにします。
92*	エラー	[ローカルスタティックルートを有効にする (Enable Local Static Route)]をオンにします。 SIP サーバグループ、および IP アドレス/ホスト名/サーバグループ名へのルートは、いずれも VXML ゲートウェイです (たとえば、vxmlgw.cisco.com) 。 [発信元へのコールの送信を有効にする (Enable Send Calls to Originator)]をオンにします。

ダイヤル番号パターン	説明	ダイヤル番号パターンのタイプ
エージェント拡張パターン。たとえば、エージェント内線の範囲が 5001 ~ 500999 の場合は 500* と入力します。	エージェントデバイス。SCC の配置モデルには適用されません。	[ローカルスタティックルートを有効にする (Enable Local Static Route)] をオンにします。 SIP サーバグループ、および IP アドレス/ホスト名/サーバグループ名へのルートは、いずれも Unified Communications Manager ゲートウェイです。 [Enable RNA Timeout for Outbound Calls] をオンにします。タイムアウトは 15 秒です。
777*	ネットワーク VRU ラベル	[ローカルスタティックルートを有効にする (Enable Local Static Route)] をオンにします。 SIP サーバグループ、および IP アドレス/ホスト名/サーバグループ名へのルートは、いずれも VXML ゲートウェイです (たとえば、vxmlgw.cisco.com) 。 [発信元へのコールの送信を有効にする (Enable Send Calls to Originator)] をオンにします。

Location-Based コール アドミッション制御

この付録のこのトピックを参照してください：[Cisco Unified Communications Manager のサービス構成設定](#), (108 ページ)



第 13 章

Cisco IOS Enterprise 音声ゲートウェイの設定

- [Cisco IOS Enterprise 音声ゲートウェイの設定, 151 ページ](#)

Cisco IOS Enterprise 音声ゲートウェイの設定

Cisco IOS 音声ゲートウェイを設定するには、次の手順を実行します。



(注) すべての設定手順を `enable > configuration terminal` モードで実行します。

手順

ステップ 1 ネットワーク インターフェイスを次のように設定します。

```
interface GigabitEthernet0/0
 ip route-cache same-interface
 duplex auto
 speed auto
 no keepalive
 no cdp enable
```

ステップ 2 グローバル設定を次のように設定します。

```
voice service voip
 no ip address trusted authenticate
 allow-connections sip to sip
 signaling forward unconditional
 sip
  rel1xx disable
  header-passing
  options-ping 60
  midcall-signaling passthru
```

ステップ 3 音声コーデック プリファレンスを次のように設定します。

```
voice class codec 1
  codec preference 1 g729r8
  codec preference 2 g711ulaw
```

ステップ 4 Unified CVP サービスと設定を次のように設定します。

```
# Default CVP Services
application
service new-call flash:bootstrap.vxml
service survivability flash:survivability.tcl
service CVPSelfService flash:CVPSelfServiceBootstrap.vxml
service ringtone flash:ringtone.tcl
service cvperror flash:cvperror.tcl
service bootstrap flash:bootstrap.tcl
service handoff flash:handoff.tcl

# Default CVP http, ivr, rtsp, mrcp and vxml settings
http client cache memory pool 15000
http client cache memory file 1000
http client cache refresh 864000
no http client connection persistent
http client connection timeout 60
http client connection idle timeout 10
http client response timeout 30
ivr prompt memory 15000
ivr asr-server rtsp://asr-en-us/recognizer
ivr tts-server rtsp://tts-en-us/synthesizer
rtsp client timeout connect 10
rtsp client timeout message 10
mrcp client timeout connect 10
mrcp client timeout message 10
mrcp client rtpsetup enable
vxml tree memory 500
vxml audioerror
vxml version 2.0
```

ステップ 5 ゲートウェイおよび sip-ua タイマーを次のように設定します。

```
gateway
media-inactivity-criteria all
timer receive-rtp 1200

sip-ua
retry invite 2
retry bye 1
timers expires 60000
timers connect 1000
reason-header override
```

ステップ 6 ダイアルピアを次のように設定します。

```
# Configure CVP survivability
dial-peer voice 1 pots
description CVP TDM dial-peer
service survivability
incoming called-number .T
direct-inward-dial

# Configure CVP Ringtone
dial-peer voice 919191 voip
description CVP SIP ringtone dial-peer
service ringtone
```

```
incoming called-number 9191T
voice-class sip rellxx disable
dtmf-relay rtp-nte
codec g711ulaw
no vad
```

```
# Configure CVP Error
dial-peer voice 929292 voip
description CVP SIP error dial-peer
service cvperror
incoming called-number 9292T
voice-class sip rellxx disable
dtmf-relay rtp-nte
codec g711ulaw
no vad
```

```
#Configure VXML leg where the incoming called-number matches the Network VRU Label
dial-peer voice 9999 voip
description Used for VRU leg
service bootstrap
incoming called-number 777T
dtmf-relay rtp-nte
codec g711ulaw
no vad
```

```
#Configure the Switch leg where
# preference is used to distinguish between sides.
# max-conn is used prevent overloading of CVP
# options-keepalive is used to handle failover
# Note: the example below is for gateways located on the A-side of a geographically
distributed deployment
```

```
dial-peer voice 70021 voip
description Used for Switch leg SIP Direct
preference 1
max-conn 225
destination-pattern xxxx..... # Customer specific destination pattern
session protocol sipv2
session target ipv4:###.###.###.### # IP Address for CVP1, SideA
session transport tcp
voice-class codec 1
voice-class sip options-keepalive up-interval 12 down-interval 65 retry 2
dtmf-relay rtp-nte
no vad
```

```
dial-peer voice 70022 voip
description Used for Switch leg SIP Direct
preference 1
```

```

max-conn 225
destination-pattern xxxx..... # Customer specific destination pattern
session protocol sipv2
session target ipv4:###.###.###.### # IP Address for CVP2, SideA
session transport tcp
voice-class codec 1
voice-class sip options-keepalive up-interval 12 down-interval 65 retry 2
dtmf-relay rtp-nte
no vad

```

```

dial-peer voice 70023 voip
description Used for Switch leg SIP Direct
preference 2
max-conn 225
destination-pattern xxxx..... # Customer specific destination pattern
session protocol sipv2
session target ipv4:###.###.###.### # IP Address for CVP1, SideB
session transport tcp
voice-class codec 1
voice-class sip options-keepalive up-interval 12 down-interval 65 retry 2
dtmf-relay rtp-nte
no vad

```

```

dial-peer voice 70024 voip
description Used for Switch leg SIP Direct
preference 2
max-conn 225
destination-pattern xxxx..... # Customer specific destination pattern
session protocol sipv2
session target ipv4:###.###.###.### # IP Address for CVP2, SideB
session transport tcp
voice-class codec 1
voice-class sip options-keepalive up-interval 12 down-interval 65 retry 2
dtmf-relay rtp-nte
no vad

```

ステップ1 ハードウェア リソース（トランスコーダ、会議ブリッジ、および MTP）を次のように設定します。

```

# Configure the voice-cards share the DSP resources located in Slot0
voice-card 0
dspfarm
dsp services dspfarm
voice-card 1
dspfarm
dsp services dspfarm
voice-card 2
dspfarm
dsp services dspfarm
voice-card 3
dspfarm
dsp services dspfarm

```

```

voice-card 4
dspfarm
dsp services dspfarm

# Point to the contact center call manager
sccp local GigabitEthernet0/0
sccp ccm ###.###.###.### identifier 1 priority 1 version 7.0 (CUCM1)
sccp ccm ###.###.###.### identifier 1 priority 1 version 7.0 (CUCM2)

# Add a SCCP group for each of the hardware resource types
sccp ccm group 1
associate ccm 1 priority 1
associate profile 2 register <gw70mtp>
associate profile 1 register <gw70conf>
associate profile 3 register <gw70xcode>

# Configure DSPFarms for Conference, MTP and Transcoder
dspfarm profile 1 conference
codec g711ulaw
codec g711alaw
codec g729r8
maximum sessions 24
associate application SCCP

dspfarm profile 2 mtp
codec g711ulaw
codec g711alaw
codec g729r8
maximum sessions software 500
associate application SCCP

dspfarm profile 3 transcode
codec g711ulaw
codec g711alaw
codec g729r8
maximum sessions 52
associate application SCCP

```

ステップ 8 (任意) SIP トランキングを設定します。

```

# Configure the resources to be monitored
voice class resource-group 1
resource cpu 1-min-avg threshold high 80 low 60
resource ds0
resource dsp
resource mem total-mem
periodic-report interval 30

# Configure one rai target for each CVP Server
sip-ua
rai target ipv4:###.###.###.### resource-group1 (CVP1A)
rai target ipv4:###.###.###.### resource-group1 (CVP2A)
rai target ipv4:###.###.###.### resource-group1 (CVP1B)
rai target ipv4:###.###.###.### resource-group1 (CVP2B)
permit hostname dns:%Requires manual replacement - ServerGroup Name defined in CVP.System.SIP
Server Groups%

```




第 14 章

Cisco Unified Communications Manager

この章には、A 側と B 側に Unified Communications Manager を設定するために実行する必要がある設定手順が含まれます。

- [Unified Communications Manager ライセンス, 158 ページ](#)
- [サービスのアクティブ化, 159 ページ](#)
- [完全修飾ドメイン名の設定, 160 ページ](#)
- [Cisco Unified Communications Manager グループの設定, 160 ページ](#)
- [会議ブリッジの設定, 161 ページ](#)
- [メディアターミネーションポイントの設定, 162 ページ](#)
- [トランスコーダの設定, 162 ページ](#)
- [メディアリソースグループの設定, 163 ページ](#)
- [メディアリソースグループリストの設定および関連付け, 164 ページ](#)
- [CTI ルートポイントの設定, 164 ページ](#)
- [アプリケーションユーザの設定, 165 ページ](#)
- [SIP オプションの設定, 165 ページ](#)
- [トランクの設定, 165 ページ](#)
- [ルートグループの設定, 166 ページ](#)

Unified Communications Manager ライセンス

ライセンスの生成と登録

手順

-
- ステップ 1 ブラウザで Unified Communications Manager を起動します (http://<CUCM パブリッシャの IP アドレス>)。
 - ステップ 2 [Cisco Prime License Manager] をクリックして、[ライセンス (License)] > [履行 (Fulfillment)] に移動します。
 - ステップ 3 [他の履行 (Other Fulfillment)] オプションの下で、[ライセンス要求の生成 (Generate License Request)] をクリックします。
 - ステップ 4 [ライセンス要求と次の手順 (License Request and Next Steps)] ウィンドウが開いたら、テキスト (PAK ID) をコピーします。
 - ステップ 5 [シスコ ライセンス登録 (Cisco License Registration)] リンクをクリックします。
 - ステップ 6 サインインし、[製品ライセンス登録に進む (Continue to Product License Registration)] をクリックします。
 - ステップ 7 [履行するシングル PAK/トークンの入力 (Enter a Single PAK or Token to fulfill)] フィールドに、PAK ID を貼り付けて、[シングル PAK/トークンの履行 (Fulfill Single PAK/Token)] をクリックします。
ライセンス ファイルが電子メール メッセージで届きます。
-

ライセンスのインストール

手順

-
- ステップ 1 電子メール メッセージからライセンス ファイルを解凍します。
 - ステップ 2 [その他の履行オプション (Other Fulfillment Options)] で、[ライセンスをファイルから履行 (Fulfill Licenses from File)] を選択します。
 - ステップ 3 [参照 (Browse)] をクリックしてライセンス ファイルを検索します。
 - ステップ 4 [インストール (Install)] をクリックし、ポップアップ ウィンドウを閉じます。
 - ステップ 5 [製品インスタンス (Product Instances)] に移動します。次に、[追加 (Add)] をクリックします。
 - ステップ 6 Cisco Unified Communications Manager パブリッシャの名前、ホスト名/IP アドレス、ユーザ名、およびパスワードを入力します。
 - ステップ 7 Unified CM の製品タイプを選択します。
 - ステップ 8 [OK] をクリックします。
 - ステップ 9 [今すぐ同期 (Synchronize Now)] をクリックします。
-

サービスのアクティブ化

サービスをアクティブ化するには、次の手順を実行します。

手順

-
- ステップ 1 <http://<CUCM パブリッシャの IP アドレス>/ccmadmin> で Cisco Unified CM の管理を開きます。
 - ステップ 2 [ナビゲーション (Navigation)] メニューから [Cisco Unified Serviceability] を選択し、[移動 (Go)] をクリックします。
 - ステップ 3 [ツール (Tools)] > [サービスのアクティベーション (Service Activation)] を選択します。
 - ステップ 4 [サーバ (Server)] ドロップダウン リストから、サービスをアクティブ化するサーバを選択し、[移動 (Go)] をクリックします。
 - ステップ 5 パブリッシャの場合、次のサービスがアクティブ化されていることを確認し、[保存 (Save)] をクリックします。
 - Cisco CallManager
 - Cisco IP Voice Media Streaming App
 - Cisco CTIManager
 - Cisco Tftp
 - Cisco Bulk Provisioning Service
 - Cisco AXL Web Service

- Cisco Serviceability Reporter
- Cisco CTL Provider
- Cisco Certificate Authority Proxy Function

ステップ 6 サブスクリイバの場合、次のサービスがアクティブ化されていることを確認し、[保存 (Save)] をクリックします。

- Cisco CallManager
- Cisco IP Voice Media Streaming App
- Cisco CTIManager
- Cisco AXL Web Service
- Cisco CTL Provider

完全修飾ドメイン名の設定

手順

-
- ステップ 1** Cisco Unified Communications Manager を開き、ログインします。
- ステップ 2** [システム (System)] > [エンタープライズパラメータ (Enterprise Parameters)] に移動します。
- ステップ 3** [クラスタ全体のドメイン設定パラメータ (Clusterwide Domain Configuration)] > [クラスタの完全修飾ドメイン名 (Cluster Fully Qualified Domain Name)] にクラスタの完全修飾ドメイン名を入力します。
- ステップ 4** [保存 (Save)] をクリックします。
-

Cisco Unified Communications Manager グループの設定

Cisco Unified Communications Manager を Unified Communications Manager グループに追加するには、次の手順を実行します。

手順

-
- ステップ 1 [ナビゲーション (Navigation)]メニューから [Cisco Unified CM Administrator] を選択し、[移動 (Go)]をクリックします。
 - ステップ 2 [システム (System)]>[Cisco Unified CM グループ (Cisco Unified CM Group)]を選択します。
 - ステップ 3 [検索 (Find)]をクリックします。 [デフォルト (Default)]をクリックします。
 - ステップ 4 2つのサブスクライバを [使用可能 (Available)]パネルから [選択済み (Selected)]パネルに移動します。
 - ステップ 5 [保存 (Save)]をクリックします。
 - ステップ 6 [リセット (Reset)]をクリックします。
-

会議ブリッジの設定

この手順は、配置の各ゲートウェイに対して実行します。

手順

-
- ステップ 1 [メディア リソース (Media Resources)]>[会議ブリッジ (Conference bridge)]を選択します。
 - ステップ 2 [新規追加 (Add New)]をクリックします。
 - ステップ 3 [Cisco IOS 会議ブリッジ (Cisco IOS Conference Bridge)]の [会議ブリッジ タイプ (Conference Bridge Type)]を選択します。
 - ステップ 4 [会議ブリッジ名 (Conference Bridge name)]フィールドに、ゲートウェイ上の設定と一致する会議ブリッジ名の固有識別子を入力します。 [Cisco IOS Enterprise 音声ゲートウェイの設定, \(151ページ\)](#) のステップ 7 を参照してください。
例では、[gw70conf] です。
Add a SCCP group for each of the hardware resource types
sccp ccm group 1
associate ccm 1 priority 1
associate profile 2 register gw70mtp
associate profile 1 register gw70conf
associate profile 3 register gw70xcode
 - ステップ 5 [デバイス プール (Device Pool)]を選択します。
 - ステップ 6 [保存 (Save)]をクリックします。
 - ステップ 7 [設定の適用 (Apply Config)]をクリックします。
-

メディアターミネーションポイントの設定

この手順は、配置の各ゲートウェイに対して実行します。

手順

-
- ステップ 1** [メディアリソース (Media Resources)]>[メディアターミネーションポイント (Media Termination Point)]を選択します。
- ステップ 2** [新規追加 (Add New)]をクリックします。
- ステップ 3** [メディアターミネーションポイント名 (Media Termination Point Name)]フィールドに、ゲートウェイ上の設定と一致するメディアターミネーションの固有識別子を入力します。 [Cisco IOS Enterprise 音声ゲートウェイの設定, \(151 ページ\)](#) のステップ 7 を参照してください。
例では、[gw70mtp] です。
- ```
Add a SCCP group for each of the hardware resource types
sccp ccm group 1
associate ccm 1 priority 1
associate profile 2 register gw70mtp
associate profile 1 register gw70conf
associate profile 3 register gw70xcode
```
- ステップ 4** [デバイスプール (Device Pool) ]を選択します。
- ステップ 5** [保存 (Save) ]をクリックします。
- ステップ 6** [設定の適用 (Apply Config) ]をクリックします。
- 

## トランスコーダの設定

この手順は、配置の各ゲートウェイに対して実行します。

### 手順

- 
- ステップ 1** [メディアリソース (Media Resources) ]>[トランスコーダ (Transcoder) ]を選択します。
- ステップ 2** [新規追加 (Add New) ]をクリックします。
- ステップ 3** [トランスコーダタイプ (Transcoder Type) ]の場合、[Cisco IOS 拡張メディアターミネーションポイント (Cisco IOS Enhanced Media Termination Point) ]を選択します。
- ステップ 4** [デバイス名 (Device Name) ]フィールドに、ゲートウェイ上の設定と一致するトランスコーダ名の固有識別子を入力します。 [Cisco IOS Enterprise 音声ゲートウェイの設定, \(151 ページ\)](#) のステップ 7 を参照してください。
- ```
# Add a SCCP group for each of the hardware resource types
sccp ccm group 1
associate ccm 1 priority 1
associate profile 2 register gw70mtp
```

```
associate profile 1 register gw70conf
associate profile 3 register gw70xcode
```

- ステップ 5** [デバイス プール (Device Pool)] フィールドで、[デフォルト (Default)] を選択します。
- ステップ 6** [保存 (Save)] をクリックします。
- ステップ 7** [設定の適用 (Apply Config)] をクリックします。

メディアリソースグループの設定

手順

- ステップ 1** [メディアリソース (Media Resources)] > [メディアリソースグループ (Media Resource Group)] を選択します。
- ステップ 2** 会議ブリッジ用のメディアリソースグループを追加します。
- [新規追加 (Add New)] をクリックします。
 - 名前を入力します。
 - [使用可能 (Available)] リストから、展開内にある入力/VXMLの組み合わせのゲートウェイごとに設定されたハードウェア会議ブリッジリソースをすべて選択し、それらをグループに追加します。
 - [保存 (Save)] をクリックします。
- ステップ 3** メディアターミネーションポイント用のメディアリソースグループを追加します。
- [新規追加 (Add New)] をクリックします。
 - 名前を入力します。
 - [使用可能 (Available)] リストから、設定されたすべてのハードウェアメディアターミネーションポイントを選択し、それらをグループに追加します。
 - [保存 (Save)] をクリックします。
- ステップ 4** トランスコーダ用のメディアリソースグループを追加します。
- [新規追加 (Add New)] をクリックします。
 - 名前を入力します。
 - [使用可能 (Available)] リストから、設定されたすべてのトランスコーダを選択し、それらをグループに追加します。
 - [保存 (Save)] をクリックします。
- ステップ 5** [保存 (Save)] をクリックします。

メディアリソースグループリストの設定および関連付け

手順

-
- ステップ 1 [メディアリソース (Media Resources)]>[メディアリソースグループリスト (Media Resource Group List)]を選択します。
 - ステップ 2 [新規追加 (Add New)]をクリックし、名前を入力します。
 - ステップ 3 メディアリソースグループリストを追加し、すべてのメディアリソースグループを関連付けます。[保存 (Save)]をクリックします。
 - ステップ 4 [システム (System)]>[デバイスプール (Device Pool)]を選択します。[検索 (Find)]をクリックします。[デフォルト (Default)]をクリックします。
 - ステップ 5 [メディアリソースグループリスト (Media Resource Group List)] ドロップダウンリストから、ステップ 2 で追加したメディアリソースグループリストを選択します。
 - ステップ 6 [保存 (Save)]をクリックします。[リセット (Reset)]をクリックします。
-

CTI ルートポイントの設定

エージェントが転送と会議に使用するコンピュータテレフォニーインテグレーション (CTI) ルートポイントを追加するには、次の手順を実行します。

手順

-
- ステップ 1 Cisco Unified CM の管理で、[デバイス (Device)]>[CTI ルートポイント (CTI Route Point)]を選択します。
 - ステップ 2 [新規追加 (Add New)]をクリックします。
 - ステップ 3 デバイス名 (例: *PCCEInternalDNs*) を設定します。
 - ステップ 4 [デバイスプール (Device Pool)]に対して [デフォルト (Default)]を選択します。
 - ステップ 5 リストからメディアリソースグループリストを選択します。
 - ステップ 6 [保存 (Save)]をクリックします。
 - ステップ 7 回線 [1] をクリックして、このルートポイントに関連付けられる電話番号を設定します。この電話番号は、内部ルーティングされるコール用に Packaged CCE で設定された任意の内部ダイヤル番号と一致するようにパターンで指定します。(たとえば、転送用や会議用)。

重要 目的のすべての内部ダイヤル番号と一致するほど柔軟で、ダイヤルプランの他の部分に対して定義した他のルートパターン向けのコールが誤って代行受信されることがないほどに十分限定されたパターンを定義します。内部コールには一意のプレフィックスを使用することを推奨します。たとえば、内部ダイヤル番号 1230000 と 1231111 がある場合、CTI ルートポイントに入力する適切な回線番号は 123XXXX になります。

アプリケーションユーザの設定

手順

-
- ステップ 1 Cisco Unified Communications Manager Administration で、[User Management] > [Application User] を選択します。
 - ステップ 2 [新規追加 (Add New)] をクリックします。
 - ステップ 3 pguser のユーザ ID を入力します。これは、コール サーバの PG セットアップに使用される名前に一致する必要があります。PIMI の追加 (CUCM PIM) , (129 ページ) を参照してください。
 - ステップ 4 [パスワード (Password)] および [パスワードの確認 (Confirm Password)] フィールドに cisco と入力します。これらは、コール サーバの PG セットアップに使用される値に一致する必要があります。
 - ステップ 5 [アクセス コントロール グループに追加 (Add to Access Control Group)] をクリックします。次に、[検索 (Find)] をクリックして、[標準 CTI によるコール モニタリングを許可 (Standard CTI Allow Call Monitoring)] および [標準 CTI 有効 (Standard CTI Enabled)] を選択します。
 - ステップ 6 [選択項目の追加 (Add Selected)] をクリックします。
 - ステップ 7 [Available Devices] から [CTI Route Point] を選択し、[Controlled Devices] のリストに追加します。
 - ステップ 8 [保存 (Save)] をクリックします。
-

SIP オプションの設定

デフォルトの SIP プロファイルを使用します。

トランクの設定

4 台の CVP コール サーバがあり、各サーバを Unified Communications Manager の SIP トランクに関連付ける必要があります。次の手順では、それぞれが異なる CVP コール サーバを対象としている 4 つの SIP トランクを設定する方法を示します。

実際のカスタマーサイト トポロジでは、代替 SIP トランク プランの使用が必要になる可能性があります。設定された SIP トランクによって 4 台の CVP コール サーバが対象となっている限りサポートされます。

手順

-
- ステップ 1** Unified Cisco CM の管理で、[デバイス (Device)] > [トランク (Trunk)] を選択します。
- ステップ 2** [新規追加 (Add New)] をクリックします。
- ステップ 3** [トランク タイプ (Trunk Type)] ドロップダウン リストから、[SIP トランク (SIP Trunk)] を選択し、[次へ (Next)] をクリックします。
- ステップ 4** [デバイス情報 (Device Information)] セクションで次の内容を入力します。
- [デバイス名 (Device Name)] フィールドに、SIP トランクの名前を入力します (たとえば、sipTrunkCVPIA)。
 - [デバイス プール (Device Pool)] ドロップダウン リストで、お客様が定義したデバイス プールを選択します。
 - リストからメディア リソース グループ リストを選択します。
 - [メディア ターミネーション ポイントが必須 (Media Termination Point Required)] チェックボックスがオフになっていることを確認します。
- ステップ 5** [SIP 情報 (SIP Information)] セクションにスクロールします。
- [接続先 (Destination)] テーブルの [行 1 (Row 1)] に、CVP サーバの IP アドレスを入力します。5060 のデフォルトの宛先ポートを受け入れます。
 - [SIP トランク セキュリティ プロファイル (SIP Trunk Security Profile)] ドロップダウン リストで、[非セキュア SIP トランク プロファイル (Non Secure SIP Trunk Profile)] を選択します。
 - [SIP プロファイル (SIP Profile)] ドロップダウン リストで、[標準 SIP プロファイル (Standard SIP Profile)] を選択します。
 - [DTMF シグナリング方式 (DTMF Signaling Method)] ドロップダウン リストで、[RFC 2833] を選択します。
- ステップ 6** [保存 (Save)] をクリックします。
- ステップ 7** [リセット (Reset)] をクリックします。
- ステップ 8** 配置内の残りのすべての CVP サーバに対して繰り返します。
-

ルート グループの設定

ルート グループを作成するには、次の手順を実行します。

手順

-
- ステップ 1 Unified Communications Manager で、[コールルーティング (Call Routing)] > [ルートハント (Route Hunt)] > [ルートグループ (Route Group)] を選択します。
 - ステップ 2 [新規追加 (Add New)] をクリックします。
 - ステップ 3 ルートグループ名を入力します。たとえば、*CVP Route Group*。
 - ステップ 4 [ルートグループに追加 (Add to Route Group)] ボタンを使用して、選択されたデバイスとしてすべての CVP トランクを追加します。
 - ステップ 5 [保存 (Save)] をクリックします。
-

ルートリストの設定

ルートグループにルートリストを追加するには、次の手順を実行します。

手順

-
- ステップ 1 Unified Communications Manager で、[コールルーティング (Call Routing)] > [ルートハント (Route Hunt)] > [ルートリスト (Route List)] を選択します。
 - ステップ 2 [新規追加 (Add New)] をクリックします。
 - ステップ 3 ルートリスト名を入力します。たとえば、*CVP Route List*。
 - ステップ 4 [Cisco Unified CM グループ (Cisco Unified Communications Manager Group)] を選択します。
 - ステップ 5 [保存 (Save)] をクリックします。
-

ルートパターンの設定

ルートリストにルートパターンを追加するには、次の手順を実行します。

手順

- ステップ 1 Unified Communications Manager で、[コールルーティング (Call Routing)] > [ルートハント (Route Hunt)] > [ルートパターン (Route Pattern)] を選択します。
 - ステップ 2 [新規追加 (Add New)] をクリックします。
 - ステップ 3 [888111000XXXX] のルートパターンを入力します。
 - ステップ 4 作成したルートリストを選択します。
 - ステップ 5 すべてのパネルのすべてのデフォルトをそのまま使用します。
 - ステップ 6 [保存 (Save)] をクリックします。
 - ステップ 7 強制承認コードに関するメッセージで [OK] をクリックします。強制承認コードは必要ありません。
-



第 15 章

展開タイプの設定

Unified Communications Manager を設定し、Unified Intelligence Center および Finesse を設定する前に、これを行ってください。

- [展開タイプの設定, 169 ページ](#)

展開タイプの設定

はじめる前に

Packaged CCE PCCE-PAC-M1 を検証し、システム インベントリを構築するワークフローには、次に示すユーザ名とパスワードを入力する必要があります。

- A 側の VMHost
- B 側の VMHost
- Cisco Unified Communications Manager の AXL
- Cisco Customer Voice Portal の CVP CLI (デフォルトの場合は wsmadmin です)
- Cisco Contact Center Enterprise の Diagnostic Framework Portico は (A 側と B 側のコール サーバおよびデータ サーバで同じである必要があります)
- Cisco Unified Intelligence Center
- Cisco Finesse

手順

- ステップ 1** `https://<IP Address>/cceadmin/Container.jsp` にアクセスします。<IP Address> は、いずれかの CCE データ サーバ (A 側または B 側の CCE データ サーバ) のアドレスです。
- ステップ 2** サインイン ページで、Active Directory ユーザ名とパスワードを入力します。

[展開の設定 (Configure Deployment)] ページが開き、デフォルトの展開タイプ [未指定 (Not Specified)] が表示されます。

ステップ 3 [Packaged CCE: CCE-PAC-M1] を選択します。

ステップ 4 A 側と B 側の VMware ホストに対する IP アドレス、ユーザ名、およびパスワードのフィールドを入力します。次に、[次へ (Next)] をクリックします。

VMware ホストは、ESXi がインストールされた 2 台の UCS サーバです。VMware ホストの IP アドレスまたはホスト名が ESXi の管理ネットワークに割り当てられます。[ユーザ名 (username)] と [パスワード (password)] フィールドは、ESXi に設定されたホストのログイン名とパスワードです。

ステップ 5 [A 側の CM 情報を指定する (Specify Side A CM Information)] ダイアログ ボックスで、次の内容を実行します。

- オン ボックス Unified Communications Manager には、ドロップダウン メニューから Unified CM パブリッシャを選択します。次に、AXL のユーザ名とパスワードを入力します。
- 外部 Unified Communications Manager の配置には、Unified CM パブリッシャの名前と IP アドレスを入力します。次に、AXL のユーザ名とパスワードを入力します。

ステップ 6 [CVP Ops コンソール サーバ情報を指定する (Specify CVP Ops Console Server Information)] ダイアログで、Web Services Manager の CLI ユーザ名とパスワードを入力します。次に、[次へ (Next)] をクリックします。

ステップ 7 [Unified CCE データ サーバ情報の指定 (Specify Unified CCE Data Server Information)] ページでは、Unified CCE Diagnostic Framework Service のユーザ名とパスワードを入力します。次に、[次へ (Next)] をクリックします。

ユーザ名とパスワードが A 側のコール サーバ、A 側のデータ サーバ、B 側のコール サーバ、および B 側のデータ サーバで同じである必要があります。

ステップ 8 Unified Intelligence Center Administration のユーザ名とパスワードを入力します。[次へ (Next)] をクリックします。

ステップ 9 Finesse Administration のユーザ名とパスワードを入力します。[次へ (Next)] をクリックします。これにより、[設定完了 (Congratulations)] 画面が開きます。

ステップ 10 [終了 (Finish)] をクリックします。これにより、[システム インベントリ (System Inventory)] ページが開きます。



第 16 章

Cisco Unified Intelligence Center

この章には、A 側と B 側に Unified Intelligence Center を設定するために実行する必要がある設定手順が含まれます。

- [Unified Intelligence Center データ ソースの設定, 171 ページ](#)
- [レポートバンドルのダウンロード, 173 ページ](#)
- [レポートバンドルのインポート, 174 ページ](#)
- [Unified Intelligence Center Administration の設定, 174 ページ](#)

Unified Intelligence Center データ ソースの設定

手順

- ステップ 1** Cisco Intelligence Center 管理者アカウント (<https://<hostname>:8444/cuic>) で Unified Intelligence Center にサインインします。
- ステップ 2** 左側のパネルの [データ ソース (Data Sources)] ドロウをクリックして、
- ステップ 3** [Unified CCE Historical データ ソース (Unified CCE Historical Data Source)] を選択します。[編集 (Edit)] をクリックして、
- [データベース ホスト (Database Host)] フィールドに、A 側の Unified CCE データ サーバの IP アドレスを入力します。
外部 AW-HDS-DDS の場合は、外部 HDS のサーバの IP アドレスを入力します。
 - [ポート (Port)] には、1433 と入力します。
 - [データベース名 (Database Name)] フィールドに、{instance}_sideA と入力します。
外部 HDS の場合は、{instance}_awdb と入力します。
 - タイムゾーンを選択します。
 - [データベース ユーザ ID (Database User ID)] に、Cisco Intelligence Center SQL ユーザ アカウントの設定時に作成した SQL Server ユーザ アカウントのユーザ名を入力します。

- f) SQL Server ユーザのパスワードを入力して確認します。
- g) [文字セット (Charset)]には、ISO-8859-1 と入力します。
- h) [インスタンス (Instance)]フィールドはブランクのままにします。
- i) [Test Connection] をクリックします。

ステップ 4 [セカンダリ (Secondary)]タブをクリックして、B 側の Unified CCE Historical データ ソースを設定します。

- a) [フェールオーバー有効 (Failover Enabled)] をクリックします。
- b) [データベース ホスト (Database Host)]フィールドに、B 側の Unified CCE データベース サーバの IP アドレスを入力します。
外部 AW-HDS-DDS の場合は、外部 AW-HDS-DDS サーバの IP アドレスを入力します。
- c) [ポート (Port)]には、1433 と入力します。
- d) 外部 HDS の場合は、{instance}_awdb と入力します。
- e) その他のフィールドを [プライマリ (Primary)]タブと同様に入力します。
- f) [Test Connection] をクリックします。
- g) [Save (保存)] をクリックします。

ステップ 5 [Unified CCE Realtime データ ソース (Unified CCE Realtime Data Source)]を選択します。

- a) [データベース ホスト (Database Host)]フィールドに、A 側の Unified CCE データ サーバの IP アドレスを入力します。
外部 AW-HDS-DDS の場合は、外部サーバの IP アドレスを入力します。
- b) [ポート (Port)]には、1433 と入力します。
- c) [データベース名 (Database Name)]フィールドに、{instance}_awdb と入力します。
- d) タイムゾーンを選択します。
- e) [データベース ユーザ ID (Database User ID)]フィールドに、Cisco Unified Intelligence Center の SQL Server ユーザアカウント用に設定したデータベース ユーザ ID のユーザ名を入力します。
- f) Cisco Unified Intelligence Center ユーザのパスワードを入力して確認します。
- g) [文字セット (Charset)]には、インストールされた SQL の文字セットを入力します。
- h) [インスタンス (Instance)]フィールドはブランクのままにします。
- i) [Test Connection] をクリックします。
- j) [保存 (Save)] をクリックします。

ステップ 6 [セカンダリ (Secondary)]タブをクリックして、B 側の Unified CCE Realtime データ ソースを設定します。

- a) [フェールオーバー有効 (Failover Enabled)] をクリックします。
- b) [データベース ホスト (Database Host)]フィールドに、B 側の Unified CCE データベース サーバの IP アドレスを入力します。
外部 AW-HDS-DDS サーバの場合は、外部 HDS のサーバの IP アドレスを入力します。
- c) [データベース名 (Database Name)]フィールドに、{instance}_awdb と入力します。
- d) その他のフィールドを [プライマリ (Primary)]タブと同様に入力します。
- e) [Test Connection] をクリックします。

f) [保存 (Save)] をクリックします。

レポートバンドルのダウンロード

次の Cisco Unified Intelligence Center レポートのバンドルは、Cisco.com からダウンロードとして入手できます (<http://software.cisco.com/download/type.html?mdfid=282163829&catid=null>)。入手できる次のバンドルをすべて表示するには、[Intelligence Center Reports] リンクをクリックしてください。

- [Realtime and Historical Transitional] テンプレート：新しいユーザに対して設計された入門的なテンプレート。これらのテンプレートは、[すべてのフィールド (All Fields)] テンプレートの簡易バージョンで、他のコンタクトセンター ソリューションで使用可能なテンプレートに類似しています。
- [Realtime and Historical All Fields] テンプレート：データベースのすべてのフィールドからデータを提供するテンプレート。これらのテンプレートは、カスタム レポート テンプレートを作成するためのベースとして特に有用です。
- [Live Data] テンプレート：コンタクトセンターのアクティビティの最新のデータを提供するテンプレート。
- [Realtime and Historical Outbound] テンプレート：アウトバウンド オプション アクティビティを報告するテンプレート。展開にアウトバウンド オプションが含まれている場合、これらのテンプレートをインポートします。
- [Realtime and Historical Cisco SocialMiner] テンプレート：SocialMiner アクティビティを報告するためのテンプレート。展開に SocialMiner が含まれている場合、これらのテンプレートをインポートします。
- [Cisco Unified Intelligence Center Admin Security] テンプレート：Cisco Unified Intelligence サーバの監査証跡、権限、およびテンプレートのオーナーを報告するためのテンプレート。

これらのバンドルのテンプレートの一部は、Cisco Packaged CCE 展開に適用されません。Packaged CCE 展開で使用されるテンプレートの詳細については、http://www.cisco.com/en/US/products/ps12586/tsd_products_support_series_home.html の『Cisco Packaged Contact Center Enterprise Reporting User Guide』を参照してください。

また、サンプルのカスタム レポート テンプレートは、Cisco Developer Network (<http://developer.cisco.com/web/ccr/documentation>) から入手可能で、次のテンプレートが含まれます。

- Cisco Unified E-Mail Interaction Manager (Unified EIM)
- Cisco Unified Web Interaction Manager (Unified WIM)
- Cisco Unified Customer Voice Portal (Unified CVP)

レポートバンドルのインポート

手順

-
- ステップ 1** 左側ペインで、[レポート (Reports)] をクリックします。
- ステップ 2** [レポートのインポート (Import Report)] をクリックします。
- ステップ 3** [ファイル名 (XML または ZIP ファイル) (File Name (XML or ZIP file))] フィールドの [参照 (Browse)] をクリックします。
- ステップ 4** ブラウズし、レポートバンドル zip ファイルを選択して、[開く (Open)] をクリックします。
- ステップ 5** ファイルを保存する場所を選択します。
- ステップ 6** [インポート (Import)] をクリックします。
- ステップ 7** [値リストのデータソース (Data Source for ValueList)] ドロップダウンリストから、使用するデータソースを選択します。
- (注) レポート定義と同じデータソースを使用しない場合だけ、値リストのデータソースを選択する必要があります。LiveData の場合、[レポート定義のデータソース (Data Source for ReportDefinition)] は、[LiveData JMS データソース (LiveData JMS DataSource)] である必要があります。[値リストのデータソース (Data Source for ValueList)] は、[UCCE Realtime] である必要があります。
- ステップ 8** [インポート (Import)] をクリックします。
-

Unified Intelligence Center Administration の設定

手順

-
- ステップ 1** Cisco Unified Intelligence Center 管理コンソールにサインインします (<http://{hostname}/oamp>)。
- ステップ 2** [クラスタ設定 (Cluster Configuration)] > [レポート設定 (Reporting Configuration)] から [Active Directory] タブを設定します。
- プライマリ Active Directory サーバのホストアドレスを入力します。
 - [ポート (Port)] のデフォルト値のままにします。
 - [マネージャの識別名 (Manager Distinguished Name)] フィールドに情報を入力します。
 - マネージャがドメインコントローラにアクセスするときに使用するパスワードを入力し、確認します。
 - [ユーザ検索ベース (User Search Base)] で、検索するドメインの識別名を指定します。
 - [ユーザ ID の属性 (Attribute for User ID)] で [sAMAccountName] を選択します。
 - UserName ID に対して少なくとも 1 つのドメインを追加します。ドメイン名の前に @ 記号を入力しないでください。

- h) ドメインをデフォルトとして設定します。
- i) [接続のテスト (Test Connection)] をクリックします。
- j) [保存 (Save)] をクリックします。

ステップ 3 すべてのデバイスの syslog を設定します。

- a) [デバイス管理 (Device Management)] > [ログおよびトレースの設定 (Log and Trace Settings)] を選択します。
- b) ホストアドレスごとに、次を実行します。
 - 関連付けられたサーバを選択します。
 - [サービスアビリティの設定の編集 (Edit Serviceability Settings)] 画面の [Syslog の設定 (Syslog Settings)] ペインで、プライマリ ホストとバックアップ ホストを設定します。 [保存 (Save)] をクリックします。

ステップ 4 すべてのデバイスのための SNMP を設定します。

- a) [ネットワーク管理 (Network Management)] > [SNMP] を選択します。
 - b) SNMP への移動、および各サーバに対して、次の内容を追加します。
 - V1/V2c コミュニティ ストリング
 - 通知先
-



第 17 章

Cisco Finesse

この章では、A 側と B 側に Cisco Finesse を設定するためにユーザが設定する必要がある設定手順について説明します。

- [Cisco Finesse プライマリ ノードでの CTI サーバの設定, 177 ページ](#)
- [Unified Contact Center Enterprise 管理およびデータ サーバの設定, 178 ページ](#)
- [Tomcat の再起動, 178 ページ](#)
- [デフォルトのデスクトップレイアウトのエージェント キュー統計情報ガジェットの無効化, 178 ページ](#)
- [ライブ データ レポート, 179 ページ](#)

Cisco Finesse プライマリ ノードでの CTI サーバの設定

手順

- ステップ 1** URL `http://<HOST ADDRESS>/cfadmin` を起動します。ここで、*hostname or IP address* は、プライマリ Finesse サーバのホスト名または IP アドレスです。
- ステップ 2** [Contact Center Enterprise CTI サーバ設定 (Contact Center Enterprise CTI Server Settings)] の下で、次の内容を更新します。
- A 側のホスト/IP アドレス (A 側のコール サーバ)
 - A 側のポート (A 側の CTI サーバ ポート) : 42027
 - Peripheral ID (CallManager PIM) : 5000
 - B 側のホスト/IP アドレス (B 側のコール サーバ)
 - B 側のポート (B 側の CTI サーバ ポート) : 43027
- ステップ 3** [保存 (Save)] をクリックします。
-

Unified Contact Center Enterprise 管理およびデータ サーバの設定

手順

-
- ステップ 1** [Contact Center Enterprise 管理およびデータ サーバの設定 (Contact Center Enterprise Administration & Data Server Settings)] の下で、次の内容を更新します。
- a) (A 側の AW サーバの) プライマリ ホスト/IP アドレス
 - b) データベース ポート : 1433
 - c) (B 側の AW サーバの) バックアップ ホスト/IP アドレス
 - d) ドメイン (必須フィールド) : Finesse が接続する Unified CCE の名前。
 - e) AW データベース名 : <ucceinstance_awdb>
 - f) ユーザ名 : データベースへのサインインに必要なドメイン ユーザ名。SQL ユーザにすることはできません。
 - g) パスワード : データベースへのサインインに必要なパスワード。
- ステップ 2** [保存 (Save)] をクリックします。
-

Tomcat の再起動

Contact Center Enterprise 管理サーバ設定でいずれかの値を変更して保存したら、プライマリ Finesse サーバで Cisco Tomcat Service を再起動する必要があります。

手順

-
- ステップ 1** Cisco Tomcat Service を停止するには、CLI コマンド **utils service stop Cisco Tomcat** を入力します。
- ステップ 2** Cisco Tomcat Service を開始するには、CLI コマンド **utils service start Cisco Tomcat** を入力します。
-

デフォルトのデスクトップ レイアウトのエージェント キュー統計情報ガジェットの無効化

エージェント キュー統計情報ガジェット (QueueStatistics.jsp) は、デフォルトのデスクトップ レイアウトの XML コードではデフォルトで無効です。ただし、このガジェットは、Packaged CCE の展開で、エージェントの役割に対応していません。ライブ データ レポート ガジェットには、エージェントの役割に対して同等の機能があります。

次の手順では、エージェントの役割のデフォルトのデスクトップ レイアウトで、エージェント キュー統計情報ガジェットを無効にする方法を説明します。Cisco Finesse の新規インストール後

に次の手順を使用します。Cisco Finesse をアップグレードしている場合は、この手順を行う前に、[デスクトップ レイアウトのアップグレード後の作業](#)、(199 ページ) を参照してください。

手順

ステップ 1 Finesse Administration Console にサインインします。

ステップ 2 [Desktop Layout] をクリックします。

ステップ 3 次のいずれかを行います。

- 次のように、XML からエージェント キュー統計情報ガジェットを削除します：
`<gadget>/desktop/gadgets/QueueStatistics.jsp</gadget>`。
- 次のように、エージェントの役割のエージェントキュー統計情報ガジェットにコメント文字
 (<!-- と -->) を追加して、ガジェットを無効にします：`<!--
 <gadget>/desktop/gadgets/QueueStatistics.jsp</gadget> -->`。

ステップ 4 [Save (保存)] をクリックします。

ライブ データ レポート

Cisco Unified Intelligence Center は、Finesse デスクトップに追加可能なライブ データのリアルタイム レポートを提供します。



(注) Finesse は、Packaged Contact Center Enterprise でのみライブ データ レポートをサポートします。

ライブ データの前提条件

デスクトップにライブ データ レポートを追加する前に、次の前提条件を満たす必要があります。

- ライブ データ レポートが設定され、Cisco Unified Intelligence Center で稼働している必要があります。
- Cisco Unified Intelligence Center および Finesse の両方で HTTP または HTTPS を使用する必要があります。一方に HTTP を使用して、もう一方に HTTPS を使用することはできません。新規インストールの後の両方のデフォルト設定は、HTTPS です。HTTP を使用する場合、Cisco Unified Intelligence Center および Finesse の両方で有効にする必要があります。Cisco Unified Intelligence Center の HTTP の有効化の詳細については、『*Administration Console User Guide for Cisco Unified Intelligence Center*』を参照してください。
- ユーザの同期が Cisco Unified Intelligence Center に対して有効になっていることを確認します。詳細については、『*Administration Console User Guide for Cisco Unified Intelligence Center*』を参照してください。

- ご使用の配置で HTTPS を使用している場合、Finesse および Cisco Unified Intelligence Center サーバにセキュリティ証明書をアップロードする必要があります。Finesse および Cisco Unified Intelligence Center の両方が、自己署名証明書を使用してインストールされます。ただし、自己署名証明書を使用する場合、ライブデータ ガジェットを使用する前に、エージェントとスーパーバイザはサインインの際に Finesse デスクトップの証明書を受け入れる必要があります。この要件を回避するために、CA 証明書を提供できます。サードパーティ証明書のベンダーから CA 証明書を取得するか、組織に対して内部で CA 証明書を作成できます。詳細については、「[参考資料](#)、[\(223 ページ\)](#)」の章のライブデータ情報を参照してください。

Finesse へのライブ レポートの追加

ここでは、Finesse デスクトップにライブデータ レポートを追加する方法について説明します。実行する手順は、配置に応じて異なります。次の表では、各手順を使用するタイミングを示します。

手順	使用するタイミング
デフォルト デスクトップ レイアウトへのライブ レポートの追加	この手順は、新規インストール後に Finesse デスクトップにライブデータ レポートを追加する場合、またはデフォルトのデスクトップのレイアウトをカスタマイズしない場合のアップグレード後に使用します。
カスタム デスクトップ レイアウトへのライブ レポートの追加	この手順は、Finesse デスクトップのレイアウトをカスタマイズした場合に使用します。
チーム レイアウトへのライブ レポートの追加	この手順は、特定のチームに対してのみデスクトップのレイアウトにライブデータ レポートを追加する場合に使用します。

デフォルト デスクトップ レイアウトへのライブ レポートの追加

Finesse デフォルト レイアウト XML には、Finesse デスクトップで使用できるライブデータ レポート ガジェットに対してコメントされた XML コードが含まれます。ガジェットは、ライブデータ ガジェットの HTTPS バージョンとライブデータ ガジェットの HTTP バージョンの2つのカテゴリに分類されます。

この手順では、デフォルトのデスクトップ レイアウトへのライブデータ レポート ガジェットの追加方法について説明します。Finesse の新規インストール後に次の手順を使用します。Finesse をアップグレードしたが、カスタム デスクトップのレイアウトがない場合は、[デスクトップ レイアウトの管理 (Manage Desktop Layout)] ガジェットで [デフォルト レイアウトを復元 (Restore Default Layout)] をクリックし、次の手順に従ってください。

手順

- ステップ 1** Finesse 管理コンソールにサインインします。
- ステップ 2** [デスクトップレイアウト (Desktop Layout)] タブをクリックします。
- ステップ 3** デスクトップのレイアウトに追加する各レポートからコメント文字 (<!-- および -->) を削除します。 エージェントが Finesse デスクトップ (HTTP または HTTPS) にアクセスするために使用する方法に一致するレポートを選択していることを確認します。
- ステップ 4** my-cuic-server を Cisco Unified Intelligence サーバの完全修飾ドメイン名と置き換えます。
- ステップ 5** 任意で、ガジェットの高さを変更します。

例 :

ライブデータ ガジェットの URL に指定される高さは、310 ピクセルです。 高さを変更する場合は、URL の `gadgetHeight` パラメータを適切な値に変更します。 たとえば、ガジェットの高さを 400 ピクセルにするには、次のようにコードを変更します。

```
<gadget>https://my-cuic-server:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?gadgetHeight=400&viewId=99E6C8E210000141000000D80A0006C4&filterId=agent.id=CL%20teamName</gadget>
```

ガジェットの高さに何も指定しない場合 (URL から 310 を削除する場合)、デフォルト値は 170 ピクセルです。

- ステップ 6** [保存 (Save)] をクリックします。
- (注) ガジェットを追加したら、Finesse デスクトップにサインインして、適切に表示されることを確認します。 多数のカラムでレポートを使用する場合、デスクトップへのアクセスに使用されるコンピュータのガジェットの高さまたは画面解像度を調整して、レポートを読みやすくしたり、スクロールしなくてもさらに行が画面に表示されるようにする必要があります場合があります。
- デスクトップのレイアウトを変更するときにサインインしているエージェントは、サインアウトしてから再度サインインして、デスクトップに変更が適用されていることを確認する必要があります。

カスタム デスクトップ レイアウトへのライブ レポートの追加

Finesse デフォルト レイアウト XML には、Finesse デスクトップで使用できるライブデータ レポート ガジェットに対してコメントされた XML コードが含まれます。 ガジェットは、ライブデータ ガジェットの HTTPS バージョンとライブデータ ガジェットの HTTP バージョンの 2 つのカテゴリに分類されます。

この手順では、カスタム デスクトップのレイアウトへのライブデータ レポート ガジェットの追加方法について説明します。

手順

- ステップ 1** Finesse 管理コンソールにサインインします。
- ステップ 2** [デスクトップ レイアウト (Desktop Layout)] タブをクリックします。
- ステップ 3** [Finesse デフォルト レイアウト XML (Finesse Default Layout XML)] をクリックして、デフォルト レイアウト XML を表示します。
- ステップ 4** Finesse デフォルト レイアウト XML から追加するレポートの XML コードをコピーします。 エージェントが HTTP を使用して Finesse にアクセスする場合、HTTP レポートの XML コードをコピーします。 HTTPS を使用する場合、HTTPS レポートの XML コードをコピーします。

例 :

HTTPS 向けのエージェント レポートを追加するには、次の内容をコピーします。

```
<gadget>https://my-cuic-server:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?gadgetHeight=310&viewId=99E6C8E210000141000000D80A0006C4&filterId=agent.id=CL%20teamName</gadget>
```

- ステップ 5** 表示させるタブのタグ内に XML を貼ります。

例 :

エージェント デスクトップの [home] タブにレポートを追加するには、次の手順を実行します。

```
<layout>
  <role>Agent</role>
  <page>
    <gadget>/desktop/gadgets/CallControl.jsp</gadget>
  </page>
  <tabs>
    <tab>
      <id>home</id>
      <label>finesse.container.tabs.agent.homeLabel</label>
      <gadgets>
        <gadget>https://my-cuic-server:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?
          gadgetHeight=310&viewId=99E6C8E210000141000000D80A0006C4&filterId=
            agent.id=CL%20teamName</gadget>
      </gadgets>
    </tab>
    <tab>
      <id>manageCall</id>
      <label>finesse.container.tabs.agent.manageCallLabel</label>
    </tab>
  </tabs>
</layout>
```

- ステップ 6** my-cuic-server を Cisco Unified Intelligence サーバの完全修飾ドメイン名と置き換えます。
- ステップ 7** 任意で、ガジェットの高さを変更します。

例 :

ライブデータ ガジェット の URL に指定される高さは、310 ピクセルです。高さを変更する場合は、URL の `gadgetHeight` パラメータを適切な値に変更します。たとえば、ガジェットの高さを 400 ピクセルにするには、次のようにコードを変更します。

```
<gadget>https://my-cuic-server:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?gadgetHeight=400&viewId=
99E6C8E210000141000000D80A0006C4&filterId=agent.id=CL%20teamName</gadget>
```

ガジェットの高さに何も指定しない場合（URL から 310 を削除する場合）、デフォルト値は 170 ピクセルです。

ステップ 8 [保存 (Save)] をクリックします。

(注) ガジェットを追加したら、Finesse デスクトップにサインインして、適切に表示されることを確認します。多数のカラムでレポートを使用する場合、デスクトップへのアクセスに使用されるコンピュータのガジェットの高さまたは画面解像度を調整して、レポートを読みやすくしたり、スクロールしなくてもさらに行が画面に表示されるようにする必要があります場合があります。

デスクトップのレイアウトを変更するときにサインインしているエージェントは、サインアウトしてから再度サインインして、デスクトップに変更が適用されていることを確認する必要があります。

チームレイアウトへのライブレポートの追加

Finesse デフォルトレイアウト XML には、Finesse デスクトップで使用できるライブデータレポートガジェットに対してコメントされた XML コードが含まれます。ガジェットは、ライブデータガジェットの HTTPS バージョンとライブデータガジェットの HTTP バージョンの 2 つのカテゴリに分類されます。

この手順では、特定のチームのデスクトップレイアウトへのライブデータレポートガジェットの追加方法について説明します。

手順

- ステップ 1** Finesse 管理コンソールにサインインします。
- ステップ 2** [デスクトップレイアウト (Desktop Layout)] タブをクリックします。
- ステップ 3** [Finesse デフォルトレイアウト XML (Finesse Default Layout XML)] をクリックして、デフォルトレイアウト XML を表示します。
- ステップ 4** Finesse デフォルトレイアウト XML から追加するレポートの XML コードをコピーします。エージェントが HTTP を使用して Finesse にアクセスする場合、HTTP レポートの XML コードをコピーします。HTTPS を使用する場合、HTTPS レポートの XML コードをコピーします。

例 :

HTTPS 向けのエージェント レポートを追加するには、次の内容をコピーします。

```
<gadget>https://my-cuic-server:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?gadgetHeight=310&viewId=99E6C8E210000141000000D80A0006C4&filterId=agent.id=CL%20teamName</gadget>
```

- ステップ 5** [チーム リソース (Team Resources)] タブをクリックします。
- ステップ 6** レポートを追加するチームのリストからチームを選択します。
- ステップ 7** <team name> エリアのリソースでは、[デスクトップ レイアウト (Desktop Layout)] タブをクリックします。
- ステップ 8** [システム デフォルトの上書き (Override System Default)] チェックボックスをオンにします。
- ステップ 9** 表示させるタブのタグ内に XML を貼ります。

例 :

エージェントデスクトップの[ホーム (home)]タブにレポートを追加するには、次の手順を実行します。

```
<layout>
  <role>Agent</role>
  <page>
    <gadget>/desktop/gadgets/CallControl.jsp</gadget>
  </page>
  <tabs>
    <tab>
      <id>home</id>
      <label>finesse.container.tabs.agent.homeLabel</label>
      <gadgets>
        <gadget>https://my-cuic-server:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?
          gadgetHeight=310&viewId=99E6C8E210000141000000D80A0006C4&filterId=
            agent.id=CL%20teamName</gadget>
        </gadget>
      </gadgets>
    </tab>
    <tab>
      <id>manageCall</id>
      <label>finesse.container.tabs.agent.manageCallLabel</label>
    </tab>
  </tabs>
</layout>
```

- ステップ 10** my-cuic-server を Cisco Unified Intelligence サーバの完全修飾ドメイン名と置き換えます。
- ステップ 11** 任意で、ガジェットの高さを変更します。

例 :

ライブデータ ガジェットの URL に指定される高さは、310 ピクセルです。高さを変更する場合は、URL の gadgetHeight パラメータを適切な値に変更します。たとえば、ガジェットの高さを 400 ピクセルにするには、次のようにコードを変更します。

```
<gadget>https://my-cuic-server:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?gadgetHeight=400&viewId=99E6C8E210000141000000D80A0006C4&filterId=agent.id=CL%20teamName</gadget>
```

ガジェットの高さにも何も指定しない場合（URL から 310 を削除する場合）、デフォルト値は 170 ピクセルです。

ステップ 12 [保存 (Save)] をクリックします。

(注) ガジェットを追加したら、Finesse デスクトップにサインインして、適切に表示されることを確認します。多数のカラムでレポートを使用する場合、デスクトップへのアクセスに使用されるコンピュータのガジェットの高さまたは画面解像度を調整して、レポートを読みやすくしたり、スクロールしなくてもさらに行が画面に表示されるようにする必要があります場合があります。

デスクトップのレイアウトを変更するときにサインインしているエージェントは、サインアウトしてから再度サインインして、デスクトップに変更が適用されていることを確認する必要があります。

Finesse のライブ データ ストック レポートの変更

この手順では、Cisco Unified Intelligence Center のライブ データ ストック レポートを変更して、Finesse デスクトップのレイアウトに変更されたレポートを追加する方法について説明します。



(注) 変更されたガジェットが確実に Finesse に表示されるようにするには、Cisco Unified Intelligence Center のレポートに対して適切な権限を与える必要があります。

手順

ステップ 1 Finesse デフォルト レイアウト XML から変更するレポートのガジェット URL をコピーして、テキスト エディタに貼り付けします。

例 :

HTTPS のエージェント レポートを変更する場合、次の URL をコピーして、テキスト エディタに貼り付けします。

```
<gadget>https://my-cuic-server:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?gadgetHeight=310&viewId=99E6C8E210000141000000D80A0006C4&filterId=agent.id=CL%20teamName</gadget>
```

ステップ 2 Cisco Unified Intelligence Center では、レポートの [編集 (Edit)] ビューで、ガジェット URL を作成するビューを選択してから、[リンク (Links)] をクリックします。

[HTML リンク (HTML Link)] フィールドには、カスタマイズされたレポートのパーマリンクを表示します。

ステップ 3 [HTML リンク (HTML Link)] フィールドからカスタマイズされたレポートのパーマリンクをコピーし、テキスト エディタに貼り付けてから、このリンクから viewID 値をコピーします。

例 :

レポートのパーマリンクから `viewId` をコピーします（この例では下線が引かれています）。

```
https://<Server Name>:8444/cuic/permalink/PermalinkViewer.htmx?  
viewId=5C90012F10000140000000830A4E5B33&linkType=htmlType&viewType=Grid
```

ステップ 4 ガジェット URL の `viewID` 値を、カスタマイズされたレポートのパーマリンクからの `viewID` 値と置き換えます。

ステップ 5 `my-cuic-server` を Cisco Intelligence Center サーバの FQDN と置き換えます。

ステップ 6 カスタマイズされたガジェット URL を [デスクトップレイアウトの管理 (Manage Desktop Layout)] ガジェットのデスクトップレイアウト XML に追加し、[Save] をクリックします。

(注) ガジェットを追加したら、Finesse デスクトップにサインインして、適切に表示されることを確認します。多数のカラムでレポートを使用する場合、デスクトップへのアクセスに使用されるコンピュータのガジェットの高さまたは画面解像度を調整して、レポートを読みやすくしたり、スクロールしなくてもさらに行が画面に表示されるようにする必要がある場合があります。

デスクトップのレイアウトを変更するときにサインインしているエージェントは、サインアウトしてから再度サインインして、デスクトップに変更が適用されていることを確認する必要があります。



第 18 章

Cisco Unified Customer Voice Portal Reporting Server

この章には、Unified Voice Portal Reporting Server を設定するために実行する必要がある設定手順が含まれます。

Courtesy Callback を使用し、Unified CVP IVR コールバック アプリケーション レポートを実行するカスタマーには、Unified CVP Reporting VM が必要です。

- [CVP OAMP での CVP Reporting Server の設定, 188 ページ](#)
- [Unified CVP レポーティング ユーザ, 188 ページ](#)
- [Cisco Unified Customer Voice Portal レポート テンプレートの取得, 188 ページ](#)
- [Cisco Unified CVP レポート データのデータ ソースの作成, 189 ページ](#)
- [Unified Intelligence Center への CVP レポート テンプレートのインポート, 191 ページ](#)

CVP OAMP での CVP Reporting Server の設定

手順

-
- ステップ 1 Unified CVP OAMP サーバで、[スタート (Start)] > [プログラム (Programs)] > [Cisco Unified Customer Voice Portal] > [Operations Console] に進みます。
 - ステップ 2 [Operations Console] ページが開いたら、ログインします。
 - ステップ 3 [デバイス管理 (Device Management)] > [Unified CVP Reporting Server] に進みます。
 - ステップ 4 [新規追加 (Add New)] をクリックします。
 - ステップ 5 Reporting Server の IP アドレスとホスト名を入力します。
 - ステップ 6 すべての Unified CVP コール サーバを [使用可能 (Available)] から [選択済み (Selected)] に移動します。
 - ステップ 7 [保存して展開 (Save and Deploy)] をクリックします。
-

Unified CVP レポートイング ユーザ

LDAP ユーザ用の Active Directory サーバのセットアップ

Unified CVP レポートイング ユーザが自分のドメイン内で定義されているユーザ名とパスワードで Unified Intelligence Center レポートイングアプリケーションにログインできるように、管理コンソールで [Active Directory] タブを設定します。

手順

-
- ステップ 1 管理アプリケーションで、[クラスタ設定 (Cluster Configuration)] > [レポート設定 (Reporting Configuration)] に移動し、[Active Directory] タブを選択します。
 - ステップ 2 このページのすべてのフィールドに入力します。ガイダンスについては、オンラインヘルプを参照してください。
 - ステップ 3 [接続のテスト (Test Connection)] をクリックします。
 - ステップ 4 接続を確認したら、[保存 (Save)] をクリックします。
-

Cisco Unified Customer Voice Portal レポート テンプレートの取得

Packaged CCE の場合は、コールバック レポートのみをインポートします。

Unified CVP レポート テンプレートをインポートするには、次の手順を実行します。

手順

- ステップ 1 Unified CVP Reporting Server で、[スタート (Start)] をクリックします。
- ステップ 2 検索ボックスで、**%CVP_HOME%\CVP_Reporting_Templates** を入力して、Enter キーを押します。
- ステップ 3 zip フォルダにコールバック レポートだけを圧縮し、Unified Intelligence Center Administration を実行するシステムにコピーします。

Cisco Unified CVP レポート データのデータ ソースの作成

データ ソースを作成するには、次の手順を実行します。

手順

- ステップ 1 **https://<CUIC パブリッシャのホスト アドレス>:8444/cuic** で Unified Intelligence Center にログインします。
- ステップ 2 [データ ソース (Data Sources)] ドロワを選択して、[データ ソース (Data Sources)] ページを開きます。
- ステップ 3 [作成 (Create)] をクリックして、[データ ソースの追加 (Add Data Source)] ウィンドウを開きます。
- ステップ 4 このページの各フィールドに次のように入力します。

フィールド	値
名前 (Name)	データ ソースの名前を入力します。 レポート作成者およびレポート定義作成者は、[データ ソース (Data Sources)] ページにアクセスできませんが、作成したカスタム レポートのデータ ソースのリストを表示することができます。これらのユーザにわかりやすいように、新しいデータ ソースに意味のある名前を付けることです。
説明 (Description)	このデータ ソースの説明を入力します。
タイプ (Type)	[Informix] を選択します。 (注) [タイプ (Type)] は、編集モードでは無効になります。

フィールド	値
データベース ホスト (Database Host)	サーバの IP アドレスまたはドメイン ネーム システム (DNS) 名を入力します。
ポート (Port)	ポート番号を入力します。通常、ポートは1526です。 このポートを CVP Reporting Server のファイアウォールで開くことが必要な場合があります ([Window ファイアウォール (Window Firewall)] > [受信の規則 (Inbound rules)] > [新規ルール (new rule)])。
データベース名 (Database name)	ストック コールバック レポートには、データベース名 <code>callback</code> を使用します。
インスタンス (Instance)	目的のデータベースのインスタンス名を指定します。デフォルトでは、これは <code>cvp</code> です。
タイムゾーン (Timezone)	データベースに保管されているデータに正しいタイムゾーンを選択します。[標準時 (Standard Time)] から [夏時間 (Daylight Savings Time)] に変更された場所では、このタイムゾーンは自動的に更新されます。
データベース ユーザ ID (Database User ID)	Unified CVP レポート データベースにアクセスするように Operations Console で設定されたレポート ユーザのユーザ ID を入力します。
[パスワード (Password)] および [パスワードの確認 (Confirm Password)]	データベース ユーザのパスワードを入力して確認します。
文字セット (Charset)	[UTF-8] を選択します。
デフォルト権限 (Default Permissions)	[マイ グループ (My Group)] および [すべてのユーザ (All Users)] グループについて、このデータソースに対する権限を表示または編集します。

- ステップ 5** [接続のテスト (Test Connection)] をクリックします。
ステータスがオンラインでない場合、エラーメッセージを確認して原因を判別し、それによってデータソースを編集します。
- ステップ 6** [保存 (Save)] をクリックして、[データソースの追加 (Add Data Source)] ウィンドウを閉じます。
新しいデータソースが、[データソース (Data Sources)] リストに表示されます。

Unified Intelligence Center への CVP レポートテンプレートのインポート

Packaged CCE は、Callback レポートのみをサポートしています。他のレポートはインポートしないでください。

手順

- ステップ 1 `https://<CUIC パブリッシャの HOST ADDRESS>:8444/cuic` で Unified Intelligence Center Web アプリケーションを起動します。
- ステップ 2 [レポート (Reports)] をクリックします。
- ステップ 3 上の Reports フォルダを右クリックし、[サブカテゴリの作成 (Create Sub-Category)] を選択します。
- ステップ 4 新しいサブカテゴリに、Unified CVP レポートのコンテナとして名前を付けます。[OK] をクリックします。
- ステップ 5 [レポートのインポート (Import Report)] をクリックします。
- ステップ 6 Unified CVP Reporting テンプレート ファイルをコピーした場所を参照し、callback.zip ファイルを選択します。[OK] をクリックします。
- ステップ 7 [保存先 (Save To)] フィールドで、ステップ 3 で行ったサブカテゴリに移動し、選択します。
- ステップ 8 [インポート (Import)] をクリックします。
- ステップ 9 [レポート定義のデータソース (Data source for Report Definition)] ドロップダウン リストから、Unified CVP Reporting データベースにアクセスするために作成したデータ ソースを選択します。
- ステップ 10 [インポート (Import)] をクリックします。



第 **IV** 部

バージョンのアップグレード

- ・ [リリース 10.5\(1\) へのアップグレード](#), 195 ページ



第 19 章

リリース 10.5(1) へのアップグレード

- [アップグレードの準備](#), 195 ページ
- [アップグレードの順序](#), 196 ページ
- [Cisco Finesse のアップグレード](#), 197 ページ
- [Cisco Unified Customer Voice Portal および Unified CVP Reporting のアップグレード](#), 200 ページ
- [Cisco Unified Contact Center データ サーバおよびコールサーバのアップグレード](#), 204 ページ
- [Cisco Unified Intelligence Center のアップグレード前](#), 212 ページ
- [Cisco Unified Intelligence Center のアップグレード](#), 214 ページ
- [Cisco Unified Communications Manager のアップグレード](#), 216 ページ
- [VMware 設定ユーティリティのアップグレード](#), 220 ページ
- [オプション : VMware vSphere ESXi のアップグレード](#), 221 ページ

アップグレードの準備

Packaged CCE リリース 9.0 またはリリース 10.0 の任意のバージョンからこのリリースの Packaged CCE にアップグレードすることができます。

NTP の設定 (NTP Configuration)

Packaged CCE は、時刻同期の信頼性を強化しました。正しく NTP を設定することは、データの報告とコンポーネント間の通信の信頼性を高めるために重要です。[NTP および時刻同期](#), (21 ページ) に示す要件を実装することが大切です。

基本設定

リリース 9.0(x) からアップグレードする場合、このリリースにアップグレードする前に、[付録 : 基本設定の更新](#), (223 ページ) の「基本設定」の章を参照してください。アップグレードしてい

る Packaged CCE 9.0(x) リリースに続いて、基本設定に追加された要件を手動で追加する必要があります。

リリース 10.0(1)以降のすべての基本コンフィギュレーションファイルの更新が自動的に適用されます。手動設定は必要ありません。

システム要件

次の表は、Release 9.0(x) 以降のハードウェアとソフトウェアの変更を示します。新規インストールについては、[システム要件](#)、[\(3 ページ\)](#) も参照してください。

項目	要件
VMware ホスト	VMware vSphere ESXi は、Packaged CCE のアップグレード前のバージョンでサポートされている最新リリースである必要があります。A 側と B 側が同じバージョンである必要があります。
Cisco Unified Communications Manager	<ul style="list-style-type: none"> • Unified CM 9.1(1) 以降のメンテナンス リリース • Unified CM 10.0(1) 以降のメンテナンス リリース
アンチウイルス ソフトウェア	次のいずれかになります。 <ul style="list-style-type: none"> • Symantec Endpoint Protection 12.1 • Trend Micro Server Protect バージョン 5.8 • McAfee VirusScan Enterprise 8.8i
ソフトウェア ライセンス	<ul style="list-style-type: none"> • Cisco Product Upgrade Tool (PUT) を使用した Unified CVP ライセンスのアップグレード • Communications Manager インターフェイスを使用した Unified Communications Manager ライセンスのアップグレード

アップグレードの順序

同じメンテナンス ウィンドウで、次の順序に従って、すべての Packaged CCE コンポーネントをアップグレードします。

- 1 Cisco Finesse をアップグレードし、Finesse 用の VM 設定ユーティリティを実行する

- 2 Unified CVP をアップグレードし、CVP 用の VM 設定ユーティリティを実行する
- 3 Unified CCE サーバをアップグレードし、Unified CCE 用の VM 設定ユーティリティを実行する
- 4 Unified Intelligence Center の VM 設定ユーティリティを実行する
- 5 展開を確認する
- 6 Cisco Unified Intelligence Center をアップグレードする
- 7 Unified Communications Manager をアップグレードし、Communications Manager 用の VM 設定ユーティリティを実行する
- 8 オプション : VMware vSphere ESXi のアップグレード

Cisco Finesse のアップグレード

アップグレードの実行

はじめる前に

プライマリ Finesse ノードのアップグレードを実行してから、セカンダリ Finesse ノードでアップグレードを実行する必要があります。

手順

-
- ステップ 1** プライマリ Finesse サーバで DRS バックアップを実行します。DRS アプリケーションにアクセスするには、[https://Finesse サーバの IP アドレス:8443/drf](https://FinesseサーバのIPアドレス:8443/drf) にブラウザを移動させます。詳細については、DRS アプリケーションで提供されるオンラインヘルプを参照してください。
- 重要** アップグレードで問題が発生し、以前のバージョンにロールバックする必要がある場合、システムを復元するために DRS バックアップが必要になります。システムの復元に DRS バックアップを使用しないと、2 番目の Finesse ノードの複製が中断し、修復できません。
- ステップ 2** 現在のレイアウトの設定を保存します。プライマリ Finesse ノード ([http://プライマリ Finesse サーバの IP アドレスまたはホスト名/cfadmin](http://プライマリFinesseサーバのIPアドレスまたはホスト名/cfadmin)) の管理コンソールにサインインします。[デスクトップ設定 (Desktop Settings)] タブの [デスクトップ レイアウトの管理 (Manage Desktop Layout)] ガジェットからレイアウト XML ファイルをコピーして、テキストファイルとしてローカルシステムに保存します。
- (注) 現在デフォルト レイアウトを実行している場合、新しいレイアウトに自動的にレイアウトがアップグレードされます。以前のバージョンからのレイアウトを使用する場合は、アップグレードが完了した後、[デスクトップ レイアウトの管理 (Manage Desktop Layout)] ガジェットにコピー アンド ペーストできます。
-

DVD/CD からの Finesse のアップグレード

手順

-
- ステップ 1 Finesse システムに SSH 接続し、プラットフォーム管理者アカウントでログインします。
 - ステップ 2 CLI から、**utils system upgrade initiate** コマンドを実行します。
 - ステップ 3 [ローカル DVD/CD (Local DVD/CD)] を選択します。utils system upgrade initiate コマンドの指示に従ってください。
 - ステップ 4 ISO イメージをマウントします。
 - ステップ 5 Automatically switch versions if the upgrade is successful プロンプトで、yes と入力して、アップグレードし、バージョンを切り替えます。
 - ステップ 6 アップグレードが完了したら、ISO をマウント解除します。ISO をマウント解除することで、CD/DVD ドライブを接続解除します。
 - ステップ 7 VMware 設定を更新するには、ユーティリティを実行します。[VMware 設定ユーティリティのアップグレード](#)、(220 ページ) を参照してください。
 - ステップ 8 Finesse Agent Desktop にサインインして、アップグレードが正常に行われたことを確認します (http://Finesse サーバの IP アドレスまたはホスト名)。
(注) Finesse が再起動したら、約 20 分待ってから、デスクトップにサインインします。
 - ステップ 9 セカンダリ Finesse サーバで繰り返し行います。
-

次の作業

デスクトップの前のレイアウトを復元する場合は、プライマリ Finesse ノードの管理コンソールにサインインします。[デスクトップレイアウトの管理 (Manage Desktop Layout)] ガジェットに保存したレイアウト XML をコピーアンドペーストします。

リモート ファイルシステムからの Finesse のアップグレード



-
- (注) Finesse のアップグレードが完了するまで待機している間、Unified CVP コンポーネントのアップグレードを開始できます。
-

手順

-
- ステップ 1** Finesse システムに SSH 接続し、プラットフォーム管理者アカウントでログインします。
- ステップ 2** CLI から、**utils system upgrade initiate** コマンドを実行します。
- ステップ 3** [SFTP] または [FTP] を選択します。
- ステップ 4** `utils system upgrade initiate` コマンドの指示に従ってください。
- ステップ 5** リモート サイトの場所およびクレデンシャルを指定します。
- ステップ 6** `Automatically switch versions if the upgrade is successful` プロンプトで、`yes` と入力して、アップグレードし、バージョンを切り替えます。
- ステップ 7** アップグレードが完了したら、ユーティリティを実行して VMware 設定を更新します。 [VMware 設定ユーティリティのアップグレード](#)、(220 ページ) を参照してください。
- ステップ 8** Finesse Agent Desktop にサインインして、アップグレードが正常に行われたことを確認します (`http://Finesse` サーバの IP アドレスまたはホスト名)。
(注) Finesse が再起動したら、約 20 分待ってから、デスクトップにサインインします。
- ステップ 9** セカンダリ Finesse サーバで繰り返し行います。
-

デスクトップ レイアウトのアップグレード後の作業

カスタム デスクトップ レイアウトを使用しない場合は、Cisco Finesse をアップグレードした後に次の作業を行います。

- 1 [Manage Desktop Layout] ガジェットで [Restore Default Layout] をクリックして、新しいデスクトップのデフォルトのレイアウトから更新をすべて追加します。
- 2 デフォルトのデスクトップ レイアウトから、エージェントの役割に対して、エージェントキュー統計情報ガジェットを無効にします。このガジェットは、Packaged CCE の展開で、エージェントの役割に対応していません。(デフォルトのデスクトップ レイアウトのエージェントキュー統計情報ガジェットの無効化、(178 ページ) を参照)。
- 3 **オプション** : エージェントの役割に対して、ライブ データ レポート ガジェットを有効にします。(デフォルト デスクトップ レイアウトへのライブ レポートの追加、(180 ページ) を参照)。

カスタム デスクトップ レイアウトを使用する場合は、Cisco Finesse をアップグレードした後に、エージェントの役割に対して、オプションのライブ データ レポート ガジェットを追加します。(カスタム デスクトップ レイアウトへのライブ レポートの追加、(181 ページ) を参照)。

Cisco Unified Customer Voice Portal および Unified CVP Reporting のアップグレード

アップグレード前の作業

手順

-
- ステップ 1** すべてのプログラムを閉じます。
- ステップ 2** サーバで実行されているサードパーティ サービスおよびアプリケーションを停止します。
- ステップ 3** Operations Console ノード以外のすべての CVP コンポーネントの、C:\Cisco\CVP フォルダをバックアップします。
- ステップ 4** 次のように Operations Console をバックアップします。
- Operations Console にログインします。
 - [Operations Console] ページで、[システム (System)] > [システム設定のエクスポート (Export System Configuration)] > [エクスポート (Export)] をクリックします。
 - 手動で sip.properties ファイルをコピーします (CVP の Operations Console は、sip.properties ファイルをエクスポートできません)。
 - CVP-OpsConsole-Backup.zip ファイルを保存します。
ネットワーク ストレージメディアまたはポータブルストレージメディアにエクスポートされた設定およびカスタム ファイルを保存します。
- ステップ 5** 次のディレクトリにあるログ ファイルをバックアップします。
- <CVP_HOME>\logs
 - <CVP_HOME>\IVXMLServer\logs
 - <CVP_HOME>\applications\<app_name>\logs
-

アップグレード

Cisco Unified CVP Operations Console のアップグレード

デフォルトのメディアファイルは、Unified CVP アップグレード時に上書きされます。ウィスパーアナウンスメントやエージェントのグリーティングなどのカスタマイズされたメディアファイルは、上書きされません。以前のリリースの書式を維持します。

手順

-
- ステップ 1** U-Law であるこのリリースの Unified CVP のデフォルトのメディア ファイルの書式を維持するには、ステップ 2 を省略して、ステップ 3 に進みます。
- ステップ 2** U-Law から A-Law の書式に変更する場合：
- C:\Cisco\CVP\conf の場所に移動します。
 - cvp_pkgs.properties ファイルで、**cvp-pkgs.PromptEncodeFormatALaw = 1** プロパティを 7 行に追加して A-Law フラグを有効にします。
(注) 「=」記号の前後にスペースを入れる必要があります。
- ステップ 3** このリリースの Unified CVP インストール DVD の CVP\Installer_Windows フォルダから、setup.exe を実行します。
- ステップ 4** 画面に表示される指示に従います。
- ステップ 5** サーバを再起動します。
- ステップ 6** VMware 設定を更新するには、ユーティリティを実行します。 [VMware 設定ユーティリティのアップグレード](#)、(220 ページ) を参照してください。
-

Cisco Unified CVP コール サーバのアップグレード

Unified CVP/VXML サーバをアップグレードする場合、Unified Call Studio も同じバージョンにアップグレードする必要があります。

手順

-
- ステップ 1** Unified CVP インストール DVD の新しいリリースの CVP\Installer_Windows フォルダから、**setup.exe** を実行します。
インストーラがアップグレード プロセスをガイドするプロンプトに従ってください。
- ステップ 2** サーバを再起動します。
- ステップ 3** VMware 設定を更新するには、ユーティリティを実行します。 [VMware 設定ユーティリティのアップグレード](#)、(220 ページ) を参照してください。
-

次の作業

- Operations Console にログインし、[一括管理 (Bulk Administration)] > [ファイル転送 (File Transfer)] > [スクリプトおよびメディア (Scripts and Media)] を選択します。
- Cisco IOS CLI コマンド **call application voice load <service_Name>** を使用して、各 Unified CVP サービスの Cisco IOS メモリにゲートウェイ ダウンロード転送ファイルをロードします。
- バックアップされたサードパーティのライブラリを復元します。

- 4 新しいバージョンのライセンスで Unified CVP サーバを再認可します。

アップグレード ファイルの取得と適用

Unified CVP サーバと Unified CVP Reporting Server には、更新されたライセンスが必要です。Operations Console は、ライセンスがなくても動作します。

ソフトウェアをアップグレードするには、契約番号を次の Cisco Product Upgrade Tool (PUT) に入力します: <http://tools.cisco.com/gct/Upgrade/jsp/index.jsp>。アップグレードする権限がある場合、ツールは Product Authorization Key (PAK) を返します。返さない場合、ツールは PAK を購入するためのオプションを表示します。

新しいライセンスは、電子メールで送信されます。

Operations Console を使用して転送できるように、ローカル的に保存します。

手順

-
- ステップ 1** Operation Console で、[一括管理 (Bulk Administration)] > [ファイル転送 (File Transfer)] > [ライセンス (Licenses)] に進みます。
- ステップ 2** [デバイスの関連付け (Device Association)] パネルで、ドロップダウン リストからデバイス タイプを選択します。たとえば、[Unified CVP Reporting Server] または [CVP コールサーバ (CVP Call Server)] を選択します。
- ステップ 3** ライセンスを与えるオブジェクトを [使用可能 (Available)] から [選択済み (Selected)] に移動します。
- ステップ 4** [ライセンス ファイル (Licenses Files)] パネルで、[新しいファイルの選択 (Select new file)] を選択してから、アップグレードライセンスを保存した場所を参照します。
- ステップ 5** [転送 (Transfer)] をクリックします。
-

Reporting Server のアップグレード

はじめる前に

- Informix データベースをバックアップします。
C:\Cisco\CVP\bin\cvpbackup.bat を実行します。これは、E:\cvp-db-backup\cvp-backup-data.gz にデータベースをバックアップします。
- スケジュールされたページをオフにします。
これを行うには、[Active Tasks] でいずれかの Unified CVP タスクをダブルクリックします。Unified CVP 関連タスクをすべて選択し、右クリックし、[Disable] を選択します。
- Reporting Server が任意のドメインに含まれず、ワークグループに含まれていることを確認します。必要に応じて、アップグレード後にドメインに追加します。

手順

-
- ステップ 1** Unified CVP の ISO イメージをマウントし、`setup.exe` を実行します。インストーラは、アップグレードプロセスをガイドします。
 - ステップ 2** パスワードの画面で、パスワードを入力し、[アップグレード (Upgrade)] をクリックします。インストール中に作成するパスワードを留めておきます。このパスワードは、設定用に Reporting Server にログインするときに必要です。
 - ステップ 3** サーバを再起動します。
 - ステップ 4** アップグレードされた Reporting Server にバックアップされたデータベースを復元します。復元するには、`c:\cisco\cvp\bin\cvprestore.bat` を実行します。
 - ステップ 5** 必要に応じて、マシンをドメインに再追加します。
 - ステップ 6** VMware 設定を更新するには、ユーティリティを実行します。 [VMware 設定ユーティリティのアップグレード](#)、(220 ページ) を参照してください。
-

ゲートウェイ Cisco IOS バージョンのアップグレード

各ゲートウェイでこの作業を行います。

手順

-
- ステップ 1** リモート TFTP サーバからフラッシュ メモリに新しいイメージをコピーして、独自の TFTP サーバの IP アドレスと Cisco IOS ファイル名が確実に指定されるようにします。
 - ステップ 2** 新しいイメージがダウンロードされたことを確認します。
 - ステップ 3** 新しいイメージを使用して起動します。新しいバージョンを使用して起動するように、ゲートウェイ設定を更新します。
 - ステップ 4** 新しいイメージを使用するように、ゲートウェイを再ロードします。
<http://www.cisco.com/en/US/docs/routers/access/as5350xm/software/configuration/guide/54ovr.html#wp1054418> も参照してください。
-

Cisco Unified Contact Center データ サーバおよびコールサーバのアップグレード

アップグレード前の作業

設定変更を無効にする

手順

アップグレード中の設定変更を無効にするには、A 側のコールサーバで次のレジストリ キーを 1 に設定します：**HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM<instance name>\Router A\Router\CurrentVersion\Configuration\Global\DBMaintenance。**

パスワードの特定

Packaged CCE PCCE-PAC-M1 を検証し、システム インベントリを構築するワークフローには、次に示すユーザ名とパスワードを入力する必要があります。

- A 側の VMHost
- B 側の VMHost
- Cisco Unified Communications Manager の AXL
- Cisco Customer Voice Portal の CVP CLI (デフォルトの場合は wsmadmin です)
- Cisco Contact Center Enterprise の Diagnostic Framework Portico は (A 側と B 側のコールサーバおよびデータサーバで同じである必要があります)

拡張データベース移行ツールのダウンロード

EDMT は、Unified CCE データベースのアップグレードに使用されるウィザードのアプリケーションです。A 側と B 側のデータサーバと外部 AW-HDS-DDS サーバのデータベースをアップグレードするときに、このツールを実行します。

手順

-
- ステップ 1 <http://www.cisco.com> に進みます。
 - ステップ 2 [サポート (Support)] をクリックします。
 - ステップ 3 [ダウンロード (Downloads)] をクリックします。
 - ステップ 4 [すべてのダウンロード カテゴリを参照する (Browse all Download Categories)] をクリックします。
 - ステップ 5 [ダウンロード ホーム (Downloads Home)] > [製品 (Products)] テーブルで、[製品 (Products)] > [カスタマー コラボレーション (Customer Collaboraton)] > [コンタクトセンター (Contact Center)] > [Cisco Unified Contact Center Enterprise] を選択します。
 - ステップ 6 [ソフトウェア タイプの選択 (Select a Software type)] ページで、[Cisco Enhanced Data Migration Tool ソフトウェア リリース (Cisco Enhanced Data Migration Tool Software Releases)] を選択し、現在のリリースに移動します。
 - ステップ 7 EDMT zip ファイルを選択します。次に、[ダウンロード (Download)] をクリックします。
 - ステップ 8 A 側の Unified CCE データ サーバにファイルをダウンロードします。
 - ステップ 9 B 側の Unified CCE データ サーバと外部 AW-HDS-DDS サーバに EDMT ファイルのダウンロードを繰り返し行います。
-

A 側のアップグレード

A 側のデータ サーバ、コール サーバ、外部 AW のサービスの停止

アップグレードを開始する前に、デスクトップから [Unified CCE サービス制御 (Unified CCE Service Control)] アイコンをクリックします。A 側のコール サーバ、A 側のデータ サーバ、外部 AW のすべてのサービスを停止し、スタートアップを [Manual] に変更します。

データ サーバ データベースのアップグレード

この手順は、リリース 9.0(x) からアップグレードする場合にのみ必要であり、リリース 10.0(x) からアップグレードする場合は実行する必要はありません。

手順

-
- ステップ 1 Microsoft SQL のバックアップを使用し、ユーティリティを復元して、ロガーデータベースのバックアップ コピーを作成します。
[http://msdn.microsoft.com/en-us/library/ms187510\(v=sql.100\).aspx](http://msdn.microsoft.com/en-us/library/ms187510(v=sql.100).aspx) の Microsoft 社の手順を参照してください。

- ステップ 2 ダウンロード ロケーションから、EDMT を開き、[次へ (Next)]をクリックします。
 - ステップ 3 [共通グラウンド (Common Ground)]を選択し、[次へ (Next)]をクリックします。
 - ステップ 4 [はい (Yes)]をクリックして、警告メッセージを承認します。
 - ステップ 5 <instanceName>_SideA または <instanceName>_SideB のデータベースを選択します。
 - ステップ 6 [Next] をクリックします。
 - ステップ 7 [移行を開始 (Start Migration)]をクリックします。
 - ステップ 8 [はい (Yes)]をクリックして、内容を確定します。
 - ステップ 9 EDMT がロガー データベースの移行を完了したら、EDMT を終了します。
 - ステップ 10 A 側の場合のみ、アウトバウンド オプションを使用する場合は、BA データベースに対して繰り返し行います。
-

データ サーバのセットアップの実行

手順

- ステップ 1 ISO をマウントします。 [ISO ファイルのマウントおよびアンマウント](#)、(83 ページ) を参照してください。
 - ステップ 2 ICM-CCE-CCHInstaller を起動し、[次へ (Next)]をクリックします。
 - ステップ 3 (任意) メンテナンス リリースを適用するには、[参照 (Browse)]をクリックして、メンテナンス リリースのソフトウェアに移動します。 [次へ (Next)]をクリックします。
 - ステップ 4 (任意) [SQL Server 2008 Security Hardening] を選択して、[次へ (Next)]をクリックします。
 - ステップ 5 パッチがインストールされている場合は、[はい (Yes)]をクリックして、セットアップがアップグレードの一環としてこれを削除することを許可します。
 - ステップ 6 表示される情報メッセージで [OK] をクリックします。
 - ステップ 7 [インストール (Install)]をクリックします。
 - ステップ 8 アップグレーが完了したら、サーバを再起動します。
 - ステップ 9 VMware 設定を更新するには、ユーティリティを実行します。 [VMware 設定ユーティリティのアップグレード](#)、(220 ページ) を参照してください。
-

Cisco Unified CCE コール サーバのセットアップの実行

手順

-
- ステップ 1 ISO をマウントします。 [ISO ファイルのマウントおよびアンマウント](#), (83 ページ) を参照してください。
 - ステップ 2 ICM-CCE-CCHInstaller を起動し、[次へ (Next)] をクリックします。
 - ステップ 3 (任意) メンテナンス リリースを適用するには、[参照 (Browse)] をクリックして、メンテナンス リリースのソフトウェアに移動します。 [次へ (Next)] をクリックします。
 - ステップ 4 表示される情報メッセージで [OK] をクリックします。
 - ステップ 5 パッチがインストールされている場合は、[はい (Yes)] をクリックして、セットアップがアップグレードの一環としてこれを削除することを許可します。
 - ステップ 6 CTI OS サーバをアップグレードする場合、Unified CCE および CTI OS サーバの両方のアップグレードが完了したら、リブートします。CTI OS サーバをアップグレードしない場合、リブートは任意です。
 - ステップ 7 CTI OS サーバをアップグレードしない場合だけ、VMware 設定 ([VMware 設定ユーティリティのアップグレード](#), (220 ページ) を参照) を更新するために、ユーティリティを実行します。CTI OS サーバをアップグレードする場合、Unified CCE および CTI OS サーバの両方のアップグレードが完了したら、ツールを実行します。
-

Cisco CTI OS サーバのセットアップの実行

このステップは、CTI OS がインストールされた場合のみ必要です。

手順

-
- ステップ 1 ISO をマウントします。 [ISO ファイルのマウントおよびアンマウント](#), (83 ページ) を参照してください。
 - ステップ 2 このリリースの CTI OS インストーラを開始し、プロンプトに従います。
 - ステップ 3 プロンプトが表示されたら、メンテナンス リリースを適用します。
 - ステップ 4 [すべてアップグレード (Upgrade All)] をクリックします。
 - ステップ 5 [はい (Yes)] をクリックします。
 - ステップ 6 [はい (Yes)] をクリックして、セットアップが完了したら再起動します。
 - ステップ 7 VMware 設定を更新するには、ユーティリティを実行します。 [VMware 設定ユーティリティのアップグレード](#), (220 ページ) を参照してください。
-

B 側のサービスと任意の外部 AW-HDS-DDS のシャットダウン

A 側を開始する前に、Unified CCE Service Control ツールを使用して、次のサービスをシャットダウンします。

- B 側の Packaged CCE データ サーバ
- B 側の Packaged CCE コール サーバ
- 任意の外部 AW-HDS-DDS サーバ

A 側の起動および動作の確認

Packaged CCE の A 側のコール サーバおよびデータ サーバでサービスを手動で起動します。

コールを発信して A 側が作用していることを確認し、確実にエージェントに正常に配信されるようにします。

B 側のアップグレード

データ サーバデータベースのアップグレード

この手順は、リリース 9.0(x) からアップグレードする場合にのみ必要であり、リリース 10.0(x) からアップグレードする場合は実行する必要はありません。

手順

-
- ステップ 1** Microsoft SQL のバックアップを使用し、ユーティリティを復元して、ロガーデータベースのバックアップ コピーを作成します。
[http://msdn.microsoft.com/en-us/library/ms187510\(v=sql.100\).aspx](http://msdn.microsoft.com/en-us/library/ms187510(v=sql.100).aspx) の Microsoft 社の手順を参照してください。
- ステップ 2** ダウンロード ロケーションから、EDMT を開き、[次へ (Next)] をクリックします。
- ステップ 3** [共通グラウンド (Common Ground)] を選択し、[次へ (Next)] をクリックします。
- ステップ 4** [はい (Yes)] をクリックして、警告メッセージを承認します。
- ステップ 5** <instanceName>_SideA または <instanceName>_SideB のデータベースを選択します。
- ステップ 6** [Next] をクリックします。
- ステップ 7** [移行を開始 (Start Migration)] をクリックします。
- ステップ 8** [はい (Yes)] をクリックして、内容を確定します。
- ステップ 9** EDMT がロガー データベースの移行を完了したら、EDMT を終了します。
- ステップ 10** A 側の場合のみ、アウトバウンド オプションを使用する場合は、BA データベースに対して繰り返し行います。
-

データ サーバのセットアップの実行

手順

-
- ステップ 1 ISO をマウントします。 [ISO ファイルのマウントおよびアンマウント](#), (83 ページ) を参照してください。
 - ステップ 2 ICM-CCE-CCHInstaller を起動し、[次へ (Next)] をクリックします。
 - ステップ 3 (任意) メンテナンス リリースを適用するには、[参照 (Browse)] をクリックして、メンテナンス リリースのソフトウェアに移動します。 [次へ (Next)] をクリックします。
 - ステップ 4 (任意) [SQL Server 2008 Security Hardening] を選択して、[次へ (Next)] をクリックします。
 - ステップ 5 パッチがインストールされている場合は、[はい (Yes)] をクリックして、セットアップがアップグレードの一環としてこれを削除することを許可します。
 - ステップ 6 表示される情報メッセージで [OK] をクリックします。
 - ステップ 7 [インストール (Install)] をクリックします。
 - ステップ 8 アップグレーが完了したら、サーバを再起動します。
 - ステップ 9 VMware 設定を更新するには、ユーティリティを実行します。 [VMware 設定ユーティリティのアップグレード](#), (220 ページ) を参照してください。
-

Cisco Unified CCE コール サーバのセットアップの実行

手順

-
- ステップ 1 ISO をマウントします。 [ISO ファイルのマウントおよびアンマウント](#), (83 ページ) を参照してください。
 - ステップ 2 ICM-CCE-CCHInstaller を起動し、[次へ (Next)] をクリックします。
 - ステップ 3 (任意) メンテナンス リリースを適用するには、[参照 (Browse)] をクリックして、メンテナンス リリースのソフトウェアに移動します。 [次へ (Next)] をクリックします。
 - ステップ 4 表示される情報メッセージで [OK] をクリックします。
 - ステップ 5 パッチがインストールされている場合は、[はい (Yes)] をクリックして、セットアップがアップグレードの一環としてこれを削除することを許可します。
 - ステップ 6 CTI OS サーバをアップグレードする場合、Unified CCE および CT IOS サーバの両方のアップグレードが完了したら、リブートします。 CTIOS サーバをアップグレードしない場合、リブートは任意です。
 - ステップ 7 CTI OS サーバをアップグレードしない場合だけ、VMware 設定 ([VMware 設定ユーティリティのアップグレード](#), (220 ページ) を参照) を更新するために、ユーティリティを実行します。 CTI OS サーバをアップグレードする場合、Unified CCE および CT IOS サーバの両方のアップグレードが完了したら、ツールを実行します。
-

Cisco CTI OS サーバのセットアップの実行

このステップは、CTI OS がインストールされた場合のみ必要です。

手順

-
- ステップ 1 ISO をマウントします。 [ISO ファイルのマウントおよびアンマウント](#)、(83 ページ) を参照してください。
 - ステップ 2 このリリースの CTIOS インストーラを開始し、プロンプトに従います。
 - ステップ 3 プロンプトが表示されたら、メンテナンス リリースを適用します。
 - ステップ 4 [すべてアップグレード (Upgrade All)] をクリックします。
 - ステップ 5 [はい (Yes)] をクリックします。
 - ステップ 6 [はい (Yes)] をクリックして、セットアップが完了したら再起動します。
 - ステップ 7 VMware 設定を更新するには、ユーティリティを実行します。 [VMware 設定ユーティリティのアップグレード](#)、(220 ページ) を参照してください。
-

B 側を起動します。

手順

B 側のコール サーバおよび B 側のデータ サーバ サービスを起動します。

外部 AW-HDS-DDS のアップグレード

外部 AW-HDS-DDS データベースのアップグレード

外部 AW HDS DDS がない場合は、アップグレード後の作業に進んでください。

この手順は、リリース 9.0(x) からアップグレードする場合にのみ必要であり、リリース 10.0(x) からアップグレードする場合は実行する必要はありません。

手順

-
- ステップ 1 Microsoft SQL のバックアップを使用し、ユーティリティを復元して、<instancename>_hds データベースのバックアップ コピーを作成します。
[http://msdn.microsoft.com/en-us/library/ms187510\(v=sql.100\).aspx](http://msdn.microsoft.com/en-us/library/ms187510(v=sql.100).aspx) の Microsoft 社の手順を参照してください。

- ステップ 2 Unified CCE Service Control を使用して、外部 AW-HDS-DDS のすべての Unified CCE サービスを停止し、スタートアップを [手動 (Manual)] に変更します。
- ステップ 3 ダウンロード ロケーションから、EDMT を開き、[次へ (Next)] をクリックします。
- ステップ 4 [共通グラウンド (Common Ground)] を選択し、[次へ (Next)] をクリックします。
- ステップ 5 [はい (Yes)] をクリックして、警告メッセージを承認します。
- ステップ 6 <instanceName>_hds データベースを選択します。
- ステップ 7 [移行を開始 (Start Migration)] をクリックします。
- ステップ 8 [はい (Yes)] をクリックして、内容を確定します。
- ステップ 9 EDMT が完了したら、EDMT を終了します。

外部 AW-HDS-DDS のセットアップの実行

手順

- ステップ 1 ISO をマウントします。 [ISO ファイルのマウントおよびアンマウント](#)、(83 ページ) を参照してください。
- ステップ 2 ICM-CCE-CCHInstaller を起動し、[次へ (Next)] をクリックします。
- ステップ 3 (任意) メンテナンス リリースを適用するには、[参照 (Browse)] をクリックして、メンテナンス リリースのソフトウェアに移動します。 [次へ (Next)] をクリックします。
- ステップ 4 (任意) [SQL Server 2008 Security Hardening] を選択して、[次へ (Next)] をクリックします。
- ステップ 5 表示される情報メッセージで [OK] をクリックします。
- ステップ 6 パッチがインストールされている場合は、[はい (Yes)] をクリックして、セットアップがアップグレードの一環としてこれを削除することを許可します。
- ステップ 7 [インストール (Install)] をクリックします。
- ステップ 8 アップグレードが完了したら、再起動します。
- ステップ 9 手動でサービスを再開します。

アップグレード後の作業

設定変更の再有効化

この手順は、一方の側に対してのみ実行します。 もう一方の側に対しては自動的に複製されません。

手順

-
- ステップ 1** アップグレード中の設定変更を有効にするには、<A/B>側のコールルータで次のレジストリ キーを 0 に設定します：**HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM\<instance name>\Router<A/B>\Router\CurrentVersion\Configuration\Global\DBMaintenance。**
- ステップ 2** 設定変更の保存を行い、設定変更が有効であることを確認します。設定変更が正常に行われている必要があります。
-

自動へのサービスの設定

次の手順を A 側のコールサーバ、A 側のデータサーバ、B 側のコールサーバ、B 側のデータサーバ、ある場合は外部 AW-HDS-DDS マシンでも繰り返し行ってください。

手順

-
- ステップ 1** [Unified CCE サービス制御 (Unified CCE Service Control)] をクリックします。
- ステップ 2** [SICM/CCE/CCH サービス制御 (SICM/CCE/CCH Service Control)] ダイアログボックスで、各サービスをクリックして、スタートアップを [自動 (Automatic)] に変更します。
-

新しい言語パックのインストール

言語パックのインストール、(229 ページ) を参照してください。

Cisco Unified Intelligence Center のアップグレード前

COP ファイルのダウンロードとインストール

アップグレードするリリースの Cisco Unified Intelligence Center の COP ファイルをダウンロードし、すべてのノードにインストールします。

手順

-
- ステップ 1** ブラウザで Cisco Unified Intelligence Center (<http://software.cisco.com/download/type.html?mdfid=282163829&i=rm>) の [Download Software] ページに移動し、Unified Intelligence Center のソフトウェアへのリンクをクリックします。

- ステップ 2** 必要なリリースのフォルダおよびサブフォルダに移動します。
- ステップ 3** Unified Intelligence Center の COP .cop.sgn ファイルを選択し、[Download] をクリックします。
- ステップ 4** [Log in] をクリックし、[Software Download] に資格情報を入力します。
- ステップ 5** COP ファイルをダウンロードしたら、COP ファイルの ReadMe ファイルに記載されているインストール手順に従います。

Cisco Unified Intelligence Center を更新するためのユーティリティの実行

検証および Cisco Unified Intelligence Center のアップグレードの前に、ユーティリティを実行して、すべてのノードで VMware 設定を更新する必要があります。 [VMware 設定ユーティリティのアップグレード](#)、(220 ページ) を参照してください。

システムの検証およびシステム インベントリの構築

手順

- ステップ 1** データ サーバで、<https://<データ サーバの IP アドレス>/cceadmin> に移動します。
- ステップ 2** [システム (System)] > [展開 (Deployment)] をクリックします。
[展開の設定 (Configure Deployment)] ページは、VM ホスト情報が欠落していることを示すエラーを表示します。これは予想どおりの結果です。
- ステップ 3** A 側と B 側の VMware ホストに対する IP アドレス、ユーザ名、およびパスワードのフィールドを入力します。次に、[次へ (Next)] をクリックします。
- ステップ 4** [A 側の CM 情報を指定する (Specify Side A CM Information)] ダイアログ ボックスで、次の内容を実行します。
- オン ボックス Unified Communications Manager には、ドロップダウン メニューから Unified CM パブリッシャを選択します。次に、AXL のユーザ名と VM のパスワードを入力します。
 - 外部 Unified Communications Manager の配置には、Unified CM パブリッシャの名前と IP アドレスを入力します。次に、AXL のユーザ名とパスワードを入力します。
- ステップ 5** [CVP Ops コンソール サーバ情報を指定する (Specify CVP Ops Console Server Information)] ダイアログで、Web Services Manager の CLI ユーザ名とパスワードを入力します。次に、[次へ (Next)] をクリックします。
- ステップ 6** [Specify Unified CCE Data Server Information] ページでは、Unified CCE Diagnostic Framework Service のユーザ名 (boston@boston.com など) とパスワードを入力します。次に、[次へ (Next)] をクリックします。

ユーザ名とパスワードが A 側のコール サーバ、A 側のデータ サーバ、B 側のコール サーバ、および B 側のデータ サーバで同じである必要があります。

- ステップ 7** Unified Intelligence Center Administration のユーザ名とパスワードを入力します。[Next] をクリックします。
- ステップ 8** Finesse Administration のユーザ名とパスワードを入力します。[Next] をクリックします。これにより、[Congratulations] 画面が開きます。
- ステップ 9** [終了 (Finish)] をクリックします。これにより、[System Inventory] ページが開きます。
- ステップ 10** SocialMiner、E-Mail and Web Interaction Manager、サードパーティ製マルチチャネルなどのマルチチャネルアプリケーションを使用している場合、次の手順で、これらを外部マシンとしてシステムインベントリに追加します。
- a) [Add Machine] をクリックします。
 - b) ドロップダウンリストから、そのタイプを選択します。
 - c) 名前を追加します。
 - d) ホスト名または IP アドレスを追加します。
 - e) [Save (保存)] をクリックします。

Cisco Unified Intelligence Center のアップグレード

アップグレード

アップグレードについて

アップグレードにかかる時間は 1 時間以内で、システムの運用を続行しながら、サーバにアップグレードソフトウェアをインストールできます。

ソフトウェアのアップグレードを開始する前に、ディザスタリカバリシステムアプリケーションを使用してシステムデータをバックアップします。DRS アプリケーションにアクセスするには、<https://Intelligence Center サーバの IP アドレス:8443/drf> にブラウザを移動させます。詳細については、DRS アプリケーションで提供されるオンラインヘルプを参照してください。

まず、コントローラノードをアップグレードして、再起動します。次に、メンバをアップグレードして、再起動します。すべてのノードが Unified Intelligence Center の同一バージョンである必要があります。

設定情報は自動的にアクティブパーティションのアップグレードされたバージョンに移行されません。

アップグレードファイルのダウンロード

手順

-
- ステップ 1 ブラウザで Cisco Unified Intelligence Center (<http://software.cisco.com/download/type.html?mdfid=282163829&i=rm>) の [Download Software] ページに移動し、Unified Intelligence Center のソフトウェアへのリンクをクリックします。
 - ステップ 2 必要なリリースのフォルダおよびサブフォルダに移動します。
 - ステップ 3 Unified Intelligence Center インストーラ .iso ファイルを選択し、[ダウンロード (Download)] をクリックします。
 - ステップ 4 [ログイン (Log in)] をクリックします。
-

DVD/CD からの Cisco Unified Intelligence Center のアップグレード

手順

-
- ステップ 1 Unified Intelligence Center システムに SSH 接続し、プラットフォーム管理者アカウントでログインします。
 - ステップ 2 ISO イメージをマウントします ([ISO ファイルのマウントおよびアンマウント](#), (83 ページ) を参照)
 - ステップ 3 CLI から、**utils system upgrade initiate** コマンドを実行します。
 - ステップ 4 [ローカル DVD/CD (Local DVD/CD)] を選択します。utils system upgrade initiate コマンドの指示に従ってください。
 - ステップ 5 Automatically switch versions if the upgrade is successful プロンプトで、yes と入力して、アップグレードし、バージョンを切り替えます。
 - ステップ 6 アップグレードが完了したら、ISO をマウント解除します。ISO をマウント解除することで、CD/DVD ドライブを接続解除します。[ISO ファイルのマウントおよびアンマウント](#), (83 ページ)
 - ステップ 7 サインインして、アップグレードが成功したことを確認します。
 - ステップ 8 サブスクライバに対して繰り返し行ってください。
 - ステップ 9 VMware 設定を更新するには、ユーティリティを実行します。[VMware 設定ユーティリティのアップグレード](#), (220 ページ) を参照してください。
-

リモート ファイル システムからの Cisco Unified Intelligence Center のアップグレード

手順

-
- ステップ 1** Cisco Unified Intelligence Center システムに SSH 接続し、プラットフォーム管理者アカウントでログインします。
- ステップ 2** CLI から、**utils system upgrade initiate** コマンドを実行します。
- ステップ 3** [SFTP] または [FTP] を選択します。
- ステップ 4** `utils system upgrade initiate` コマンドの指示に従ってください。
- ステップ 5** リモート サイトの場所およびクレデンシャルを指定します。
- ステップ 6** `Automatically switch versions if the upgrade is successful` プロンプトで、`yes` と入力して、アップグレードし、バージョンを切り替えます。
- ステップ 7** サインインして、アップグレードが成功したことを確認します。
- ステップ 8** サブスクライバに対して繰り返し行ってください。
- ステップ 9** VMware 設定を更新するには、ユーティリティを実行します。 [VMware 設定ユーティリティのアップグレード](#)、(220 ページ) を参照してください。
-

Cisco Unified Communications Manager のアップグレード

アップグレード前の作業

Cisco Unified Communications Manager をアップグレードする前に、次の内容を実行する必要があります。

- 新しいリリース用の必要なライセンス ファイルがあることを確認します。
- システムをバックアップします。詳細については、<http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html> の『*Disaster Recovery System Administration Guide*』を参照してください。
- Cisco.com からアップグレード ファイルを取得し、FTP または SFTP サーバに保存します。アップグレードファイルにアクセスする際に入力するディレクトリ名とファイル名は、大文字と小文字が区別されるため、注意してください。詳細については、<http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-release-notes-list.html> で Cisco Unified Communications Manager のリリース ノートを参照してください。

アップグレード

DVD/CD からの Cisco Unified Communications Manager のアップグレード

まず、パブリッシャノードをアップグレードします。次に、サブスクリバをアップグレードします。

手順

-
- ステップ 1 Cisco Unified Communications Manager システムに SSH 接続し、プラットフォーム管理者アカウントでログインします。
 - ステップ 2 CLI から、**utils system upgrade initiate** コマンドを実行します。
 - ステップ 3 [ローカル DVD/CD (Local DVD/CD)] を選択します。utils system upgrade initiate コマンドの指示に従ってください。
 - ステップ 4 ISO イメージをマウントします (ISO ファイルのマウントおよびアンマウント、(83 ページ) を参照)。
 - ステップ 5 Automatically switch versions if the upgrade is successful プロンプトで、yes と入力します。
 - ステップ 6 アップグレードが完了したら、ISO をマウント解除します。ISO をマウント解除することで、CD/DVD ドライブを接続解除します。mount-iso-10
 - ステップ 7 アップグレードが成功したことをサインイン画面で確認します。
 - ステップ 8 パブリッシャのアップグレードが完了したら、2つのサブスクリバに対してアップグレードを繰り返します。
-

リモート ファイル システムからの Cisco Unified Communications Manager のアップグレード

手順

-
- ステップ 1 Cisco Unified Communications Manager システムに SSH 接続し、プラットフォーム管理者アカウントでログインします。
 - ステップ 2 CLI から、**utils system upgrade initiate** コマンドを実行します。
 - ステップ 3 [SFTP] または [FTP] を選択します。
 - ステップ 4 utils system upgrade initiate コマンドの指示に従ってください。
 - ステップ 5 リモート サイトの場所およびクレデンシャルを指定します。
 - ステップ 6 Automatically switch versions if the upgrade is successful プロンプトで、yes と入力します。
 - ステップ 7 アップグレードが成功したことをサインイン画面で確認します。
 - ステップ 8 パブリッシャのアップグレードが完了したら、2つのサブスクリバに対してアップグレードを繰り返します。
-

ソフトウェア バージョンの切り替え

Unified Communications Manager をアップグレードしたら、アクティブなソフトウェアのバージョンが、アップグレードしたバージョンであることを確認します。そのバージョンが非アクティブである場合は、この手順での指示に従い、バージョンを切り替えます。

バージョンを切り替えるとシステムが再起動し、非アクティブなソフトウェアがアクティブになります。システムの再起動には、最大で 15 分ほどかかります。

パブリッシャ ノードを先に切り替える必要があります。



注意

この手順を実行すると、システムが再起動し、一時的に使用できない状態になります。

手順

-
- ステップ 1** <https://<Unified Communications Manager machine name>/cmplatform> から、Cisco Unified Communications Operating System Administration にログインします。
- ステップ 2** [設定 (Settings)] > [バージョン (Version)] の順で選択します。
- ステップ 3** アクティブなソフトウェアと非アクティブなソフトウェアのバージョンを確認します。
- ステップ 4** アップグレードしたバージョンがアクティブなバージョンでない場合は、次を実行します。
- [バージョンの切り替え (Switch Versions)] を選択して、バージョンを切り替え、システムを再起動します。
 - VMware 設定を更新するには、ユーティリティを実行します。 [VMware 設定ユーティリティのアップグレード](#)、(220 ページ) を参照してください。
 - A 側のサブスクライバおよび B 側のサブスクライバに対して繰り返し行ってください。
-

コール サーバでの JTAPI のアップグレード

Unified Communications Manager をアップグレードする場合、A 側と B 側のコール サーバに存在する JTAPI クライアントもアップグレードする必要があります。

新しい JTAPI クライアントは Unified Communications Manager Administration アプリケーションを使用してインストールします。

手順

-
- ステップ 1** 各コール サーバから古い JTAPI クライアントをアンインストールします。
- PG1A/PG1B を停止します。
 - [コントロール パネル (Control Panel)] > [プログラム (Programs)] に進みます。

- c) 次のすべてのプロンプトに従って、JTAPI クライアントをアンインストールします。
- ステップ 2** Unified Communications Manager Administration アプリケーションを起動するには、各コールサーバの Web ブラウザに次の URL を入力します : **https://<Unified Communications Manager machine name>/ccmadmin**。
- ステップ 3** Unified Communications Manager のインストールと設定時に作成したユーザ名とパスワードを入力します。
- ステップ 4** [アプリケーション (Application)] > [プラグイン (Plug-ins)] を選択します。
- ステップ 5** [検索 (Find)] をクリックして、アプリケーションの一覧を表示します。
- ステップ 6** Windows 対応の Cisco JTAPI 32-bit Client の隣のダウンロードリンクをクリックします。
- ステップ 7** [このプログラムを現在の場所から実行する (Run this program from its current location)] を選択します。 [OK] をクリックします。
- ステップ 8** [セキュリティ上の警告 (Security Warning)] ボックスが表示されたら、[はい (Yes)] をクリックしてインストールします。
- ステップ 9** Cisco TFTP サーバの IP アドレスが求められたら、Unified Communications Manager Publisher の IP アドレスを入力します。 [次へ (Next)] をクリックします。
- ステップ 10** 残りのセットアップウィンドウで [次へ (Next)] または [続行 (Continue)] を選択します。 デフォルトのインストールパスを受け入れます。
- ステップ 11** [完了 (Finish)] をクリックして PG を起動します。
-

ライセンス

アップグレードライセンス

はじめる前に

[ライセンスの生成と登録](#), (158 ページ) の手順を使用して、ライセンスを生成します。

手順

-
- ステップ 1** 電子メール メッセージからライセンス ファイルを解凍します。
- ステップ 2** ブラウザで Unified Communications Manager を起動します (<http://<CUCM パブリッシャの IP アドレス>>)。
- ステップ 3** [Cisco Prime License Manager] をクリックして、[License] > [Fulfillment] に移動します。
- ステップ 4** [その他の履行オプション (Other Fulfillment Options)] で、[ライセンスをファイルから履行 (Fulfill Licenses from File)] を選択します。
- ステップ 5** [参照 (Browse)] をクリックしてライセンス ファイルを検索します。
- ステップ 6** [インストール (Install)] をクリックし、ポップアップ ウィンドウを閉じます。
- ステップ 7** [製品インスタンス (Product Instances)] に移動します。古いインスタンスを削除します。次に、[追加 (Add)] をクリックします。
- ステップ 8** Cisco Unified Communications Manager パブリッシャの名前、ホスト名/IP アドレス、ユーザ名、およびパスワードを入力します。
- ステップ 9** Unified CM の製品タイプを選択します。
- ステップ 10** [OK] をクリックします。
- ステップ 11** [今すぐ同期 (Synchronize Now)] をクリックします。
-

VMware 設定ユーティリティのアップグレード

この手順は、リリース 9.0(x) からアップグレードする場合にのみ必要であり、リリース 10.0(x) からアップグレードする場合は実行する必要はありません。

アクティブでない ESXi ホスト サーバのアップグレード中にこのユーティリティを実行します。このツールは次のように VM を検証し、更新します。

- VM の電源がオンになっていることを確認します。
- 必要に応じて、VMware ツールを更新します。
- 必要に応じて、ゲスト VM のオペレーティングシステムの設定に一致するように VMware オペレーティングシステム設定を変更します。
- 必要に応じて、Packaged CCE 仕様に一致するように VM メモリ割り当ての設定を変更します。
- 必要に応じて、Cisco Unified Communications Manager、CCE、および CVP VM のネットワーク アダプタ タイプを、サポートされているタイプに変更します。
- 必要に応じて、Finesse VM のネットワーク アダプタ タイプを、サポートされているタイプに変更します。
- 外部の継続的なルートを削除し、NIC が変更された後に再び追加します。

はじめる前に

すべての仮想マシンに電源が投入され、VMware ツールがインストールされている必要があります。

手順

-
- ステップ 1** [Packaged CCE Download Software] ページ (<http://software.cisco.com/download/type.html?mdfid=284360381&i=rm>) の、[Packaged Contact Center Enterprise Deployment Scripts] リンクから、UpgradeVMwareSettings zip をダウンロードします。zip ファイルをローカルで解凍します。
- ステップ 2** コマンドラインから、`java -jar UpgradeVMwareSettings-10.5.jar` を実行します。
- ステップ 3** A 側と B 側の ESXi ホストの IP アドレスを入力します。
- ステップ 4** ESXi ホストにルートレベルアクセス用のユーザ名とパスワードを入力します。これは、そのホストのすべての VM のリストを表示します。番号で表示されるすべての仮想マシンの概要が、修正する必要があるツールを示すメッセージとともに表示されます。
- ステップ 5** 更新するサーバの番号を入力します。一度に 1 つの VM を更新する必要があります。変換プロセスの結果が画面に表示され、`vmwareConversion.log` の結果ディレクトリに保存されます。
- ステップ 6** Windows サーバを更新する場合は、VM のユーザ名とパスワードを入力します。
- ステップ 7** コールサーバまたはデータサーバの更新を実行した後、ネットワークのバインディング順序が正しいことを確認します。ツールが正しいバインディング順序を設定できなかった場合は、次のメッセージがコンソールとログに表示されます。**The Utility is unable to fix the binding order for the network.** [コールサーバおよびデータサーバのネットワークアダプタの設定, \(91 ページ\)](#) のバインディング順序の手順を参照してください。
-

オプション : VMware vSphere ESXi のアップグレード

VMware vCenter Server を展開で使用する場合は、VMware vCenter Server をアップグレードしてから、VMware vSphere ESXi をアップグレードします。

A 側と B 側のサーバで、このリリースの Packaged CCE でサポートされる最新バージョンに、VMware vSphere ESXi をアップグレードします。Packaged CCE では、VMware のマニュアル (<https://www.vmware.com/support/pubs/>) に記載されている標準的なアップグレード手順を使用します。



付録

A

参考資料

- [基本設定の更新, 223 ページ](#)
- [言語パックのインストール, 229 ページ](#)
- [簡易ネットワーク管理プロトコル, 229 ページ](#)
- [Cisco Unified Communications Manager のサービス構成設定, 230 ページ](#)
- [ライブデータの証明書, 231 ページ](#)

基本設定の更新

ここでは、リリース 9.0(1) の初期基本設定に続く基本コンフィギュレーションファイルの更新を示します。古い基本設定がある場合は、以降のバージョンにアップグレードする前に、欠落している設定項目を手動で適用する必要があります。たとえば、リリース 9.0(1) からリリース 9.0(4) にアップグレードする場合、リリース 9.0(2) およびリリース 9.0(3) の基本設定の変更を手動で更新する必要があります。手動で更新するには、適切な Configuration Manager のツールにアクセスできるように Packaged CCE から展開タイプを変更します。

リリース 10.0(1) からアップグレードする場合、基本設定の変更は必要ありません。



(注) 最新の基本設定をインストールすると、現在の設定情報が削除されます。

リリース 10.0(1) 以降のすべての基本コンフィギュレーションファイルの更新が自動的に適用されます。手動設定は必要ありません。たとえば、リリース 9.0(2) からリリース 10.5(1) にアップグレードする場合、リリース 9.0(3) およびリリース 9.0(4) の基本設定の変更を手動で更新する必要はありません。

リリース 9.0(2) の基本設定の変更

[拡張コール変数 (Expanded Call Variables)] --- 次の 2 つの ECC 変数を削除し、次のパラメータの変更で再度追加します。

1 Name = user.microapp.ToExtVXML

- Maximum length = 60
- Array = checked
- Maximum array size = 4

2 Name = user.microapp.FromExtVXML

- Maximum length = 60
- Array = checked
- Maximum array size = 4

リリース 9.0(3) の基本設定の変更

[Enterprise Route and Enterprise Skill Groups] : すべてを削除します。

[ラベル (Label)] --- 次のラベルを追加します。

- Label = 6661111000
- Label type = Normal
- Target Type (filter)= Network_VRU
- Network target = CVP_Network_VRU
- Customer = <None>

[メディアルーティングドメイン (Media Routing Domain)] --- 次のように4つのメディアルーティングドメインを追加します。

1 Name = Cisco_BC

- Media Class = CIM_BC
- Task life = 300
- Task start timeout = 30
- Task Max Duration = 28800
- Calls in Queue Max = 50
- Calls in Queue Max per call type = 50
- Calls in Queue Max time in queue = 28800
- Service level threshold = 30
- Service level type = Ignore abandoned calls
- Interruptible = checked

2 Name = Cisco_EIM

- Media Class = CIM_EIM

- Task life = 300
- Task start timeout = 30
- Task Max Duration = 28800
- Calls in Queue Max = 50
- Calls in Queue Max per call type = 50
- Calls in Queue Max time in queue = 28800
- Service level threshold = 30
- Service level type = Ignore abandoned calls
- Interruptible = checked

3 Name = Cisco_EIM_Outbound

- Media Class = CIM_EIM_Outbound
- Task life = 300
- Task start timeout = 30
- Task Max Duration = 28800
- Calls in Queue Max = 50
- Calls in Queue Max per call type = 50
- Calls in Queue Max time in queue = 28800
- Service level threshold = 30
- Service level type = Ignore abandoned calls
- Interruptible = checked

4 Name = Cisco_WIM

- Media Class = CIM_WIM
- Task life = 300
- Task start timeout = 30
- Task Max Duration = 28800
- Calls in Queue Max = 50
- Calls in Queue Max per call type = 50
- Calls in Queue Max time in queue = 28800
- Service level threshold = 30
- Service level type = Ignore abandoned calls
- Interruptible = checked

[Network Trunk Group] --- 次のネットワーク トランク グループを追加します。

- Name = GENERIC
- Description = null

[Trunk Group] --- 次の 12 のトランク グループをネットワーク トランク グループの GENERIC に追加します。

- 1 Peripheral = CVP_PG_1A
 - Peripheral number = 100
 - Peripheral Name = 100
 - Name = CVP_PG_1A.100
 - Trunk count = 0
- 2 Peripheral = CVP_PG_1A
 - Peripheral number = 200
 - Peripheral name = 200
 - Name = CVP_PG_1A.200
 - Peripheral ID = 5001
 - Trunk count = 0
- 3 Peripheral = CVP_PG_1A
 - Peripheral number = 300
 - Peripheral name = 300
 - Name = CVP_PG_1A.300
 - Trunk count = 0
- 4 Peripheral = CVP_PG_1B
 - Peripheral number = 100
 - Peripheral name = 100
 - Name = CVP_PG_1B.100
 - Trunk count = 0
- 5 Peripheral = CVP_PG_1B
 - Peripheral number = 200
 - Peripheral name = 200
 - Name = CVP_PG_1B.200
 - Trunk count = 0
- 6 Peripheral = CVP_PG_1B

- Peripheral number = 300
- Peripheral name = 300
- Name = CVP_PG_1B.300
- Trunk count = 0

7 Peripheral = CVP_PG_2A

- Peripheral number = 100
- Peripheral name = 100
- Name = CVP_PG_2A.100
- Trunk count = 0

8 Peripheral = CVP_PG_2A

- Peripheral number = 200
- Peripheral name = 200
- Name = CVP_PG_2A.200
- Trunk count = 0

9 Peripheral = CVP_PG_2A

- Peripheral number = 300
- Peripheral name = 300
- Name = CVP_PG_2A.300
- Trunk count = 0

10 Peripheral = CVP_PG_1B

- Peripheral number = 100
- Peripheral name = 100
- Name = CVP_PG_2B.100
- Trunk count = 0

11 Peripheral = CVP_PG_1B

- Peripheral number = 200
- Peripheral name = 200
- Name = CVP_PG_2B.200
- Trunk count = 0

12 Peripheral = CVP_PG_1B

- Peripheral number = 300

- Peripheral name = 300
- Name = CVP_PG_2B.300
- Trunk count = 0

リリース 9.0(4) の基本設定の変更

[エージェント ターゲティング ルール (Agent Targeting Rule)] --- 次のルールを追加します。

Name = AgentExtensions

- Peripheral = CUCM_PG_1
- Rule type = Agent Extension
- Translation route id = <None>
- Agent extension prefix = null
- Agent extension length = 1
- Routing client:
 - CUCM_PG_1
 - CVP_PG_1A
 - CVP_PG_1B
 - CVP_PG_2A
 - CVP_PG_2B
 - 発信
 - マルチチャネル
- 内線範囲 (低 ~ 高) :
 - 000---999
 - 0000---9999
 - 00000---99999
 - 000000---999999
 - 0000000---9999999
 - 00000000---99999999
 - 000000000---999999999
 - 0000000000---9999999999

[ラベル (Label)] --- ルーティング クライアント CVP_PG_1A、CVP_PG1B、CVP_PG_2A および CVP_PG2B のラベル属性を 7777777777 に変更します。

[メディアルーティングドメイン (Media Routing Domain)] --- 次のように 9.0(3) に追加された 3 つのメディアルーティングドメインを変更します。

1 Name = Cisco_BC

- Change Interruptible to ununchecked.

2 Name = Cisco_EIM

- Calls in Queue Max を 15000 に変更します。

3 Name = Cisco_WIM

- Calls in Queue Max を 5000 に変更します。

言語パックのインストール

カスタマーが、デフォルト (英語) ではなくこれらの言語の 1 つを必要とする場合は、[Unified Contact Center Download Software] ページから Packaged CCE 言語パックの実行可能ファイルをダウンロードできます。

言語パックのインストール

言語パックを、CCE データサーバ (A 側および B 側) および任意の外部 HDS システムにインストールします。言語パックをインストールすると、[Unified Web Administration Sign-In] ページにすべての使用可能な言語をリストする言語ドロップダウンメニューが表示されます。ある言語でユーザインターフェイスとオンラインヘルプを表示するには、その言語を選択します。



重要

オフピーク時間にインストールしてください。CCE データサーバおよび外部 HDS システムは、言語パックのインストール中は使用できません。

言語パックのアンインストール

カスタマーは、Windows の [コントロールパネル (Control Panel)] > [プログラムと機能 (Programs and Features)] > [プログラムのアンインストールまたは変更 (Uninstall or change a program)] から言語パックをアンインストールできます。

簡易ネットワーク管理プロトコル

簡易ネットワーク管理プロトコル (SNMP) を使用すると、ネットワークデバイス間での管理情報を簡単に交換できるため、管理者はネットワークパフォーマンスを管理し、ネットワークの問題を解決できます。SNMP コミュニティストリング、ユーザ、およびネットワーク宛先は、Cisco Unified Serviceability で設定されます。

Unified Serviceability は、Cisco Unified Communications ソリューション ツール内の [ナビゲーション (Navigation)] ドロップダウンから開くツールの 1 つです。また、<http://x.x.x.x/cmsservice/> と入力して Unified Serviceability にアクセスすることもできます (x.x.x.x はパブリッシャの IP アドレスです)。

コミュニティ スtring

SNMP エージェントは、セキュリティの提供にコミュニティ スtring を使用します。管理情報ベース (MIB) にアクセスするには、コミュニティ スtring を設定する必要があります。Cisco Serviceability 管理インターフェイスに新しいコミュニティ スtring を追加します。

コミュニティ スtring は、次を使用して設定します。

- サーバ 1 台
- 最大 32 文字の名前
- 任意のホストまたは指定したホストからの SNMP パケットを受け入れる設定
- アクセス権限 (readonly、readwrite、readwritenotify、notifyonly、readnotifyonly、および none)
- クラスタ内のすべてのノードにコミュニティ スtring を適用する設定

通知宛先

イベント発生時の SNMP 通知イベントの配信のための通知宛先を追加します。Cisco Serviceability 管理インターフェイスで通知宛先を追加およびメンテナンスします。

通知宛先は、次を使用して設定します。

- サーバ 1 台
- トラップ宛先のホスト IP アドレス
- ポート番号
- SNMP バージョン (V1 または V2c)
- ホストが生成する通知メッセージで使用するコミュニティ スtring 名
- 通知の種類
- クラスタ内のすべてのノードに通知宛先設定を適用する設定

Cisco Unified Communications Manager のサービス構成設定

ロケーションベースのコールアドミッション制御 (CAC) は、Unified CCE 支社コールフローモデル (別名、集中型モデル) で使用されます。これは、すべてのサーバ (Unified CVP、Unified CCE、Unified Communications Manager、および SIP プロキシサーバ) が 1 つまたは 2 つのデータセンターおよびそれぞれの支社に集中化されることを意味します。

次の設定パラメータを設定して、Unified Communications Manager がコールの発信ロケーションとしての Unified CVP ではなく、入力ゲートウェイを使用するようにします。これらの設定により、CAC が発信側エンドポイントと電話機の場所に基づいて適切に調整されます。

手順

-
- ステップ 1 Unified CM サービスパラメータの [不明な TCP 接続を受け入れる (Accept Unknown TCP connection)] を設定します。
 - ステップ 2 Unified CM サービスパラメータの [1720 をリッスンする GK 制御トランク (GK controlled trunk that will listen to 1720)] を [なし (None)] に設定します。
 - ステップ 3 Unified CM のゲートウェイ デバイスとして Unified CVP を定義しないでください。
 - ステップ 4 Unified CM のゲートウェイ デバイスとして入力ゲートウェイを定義します。デバイスに正しい場所を割り当てます。
-

ライブデータの証明書

Finesse および Cisco Unified Intelligence Center で HTTPS を使用する場合、Finesse および Cisco Unified Intelligence Center で提供される自己署名証明書を使用して、サードパーティ ベンダーから CA 証明書を取得してインストールするか、内部で CA 証明書を作成する必要があります。この付録の手順は、自己署名証明書を使用する方法、または CA 証明書を作成してアップロードする方法について説明します。

ライブデータの自己署名証明書の追加

Finesse および Cisco Unified Intelligence Center の両方が、自己署名証明書を使用してインストールされます。次の手順では、これらの自己署名証明書を使用します。ただし、自己署名証明書を使用する場合、ライブデータ ガジェットを使用する前に、エージェントはサインインの際に Finesse デスクトップの証明書を受け入れる必要があります。この要件を回避するために、CA 証明書を提供できます。サードパーティ証明書のベンダーから CA 証明書を取得するか、組織に対して内部で CA 証明書を作成できます。

手順

-
- ステップ 1 Cisco Unified Intelligence Center の Cisco Unified Operating System Administration にサインインします (<http://Cisco Unified Intelligence Center サーバのホスト名/cmplatform>) 。
 - ステップ 2 [セキュリティ (Security)] メニューから、[証明書の管理 (Certificate Management)] を選択します。
 - ステップ 3 [検索 (Find)] をクリックします。
 - ステップ 4 [tomcat.pem] をクリックします。

- tomcat.pem がリストにない場合は、[新規作成 (Generate New)] をクリックして、[証明書の名前 (Certificate Name)] ドロップダウンリストから [tomcat] を選択します。
- ステップ 5** [ダウンロード (Download)] をクリックして、デスクトップにファイルを保存します。Cisco Unified Intelligence Center パブリッシャと Cisco Unified Intelligence Center サブスクライバのホスト名を含む証明書をダウンロードする必要があります。
- ステップ 6** プライマリ Finesse サーバの Cisco Unified Operating System Administration にサインインします ([http://Finesse サーバのホスト名/cmplatform](http://Finesseサーバのホスト名/cmplatform))。
- ステップ 7** [セキュリティ (Security)] メニューから、[証明書の管理 (Certificate Management)] を選択します。
- ステップ 8** [証明書のアップロード (Upload Certificate)] をクリックします。
- ステップ 9** [証明書の名前 (Certificate Name)] ドロップダウンリストから、[tomcat-trust] を選択します。
- ステップ 10** [Choose file] をクリックして、tomcat.pem ファイル (Cisco Unified Intelligence Center のパブリッシャとサブスクライバの証明書) のロケーションを参照してください。
- ステップ 11** [ファイルのアップロード (Upload File)] をクリックします。
- ステップ 12** Cisco Tomcat を再起動します。

ライブデータの CA 証明書の取得およびアップロード

Cisco Unified Intelligence Center パブリッシャ サーバおよび Finesse プライマリ サーバの両方で、次の手順を実行する必要があります。Cisco Unified Communications オペレーティングシステムの管理から Certificate Management ユーティリティを使用します。

[Cisco Unified Communications オペレーティングシステムの管理 (Cisco Unified Communications Operating System Administration)] を開いて、ブラウザに次の URL を入力します。

[https://Finesse または Cisco Unified Intelligence Center サーバのホスト名/cmplatform](https://FinesseまたはCiscoUnifiedIntelligenceCenterサーバのホスト名/cmplatform)

手順

- ステップ 1** CSR を作成します。
- [セキュリティ (Security)] > [証明書の管理 (Certificate Management)] > [CSR の作成 (Generate CSR)] を選択します。
 - [証明書の名前 (Certificate Name)] ドロップダウンリストで、[tomcat] を選択します。
 - [CSR の作成 (Generate CSR)] をクリックします。
- ステップ 2** CSR をダウンロードします。
- [セキュリティ (Security)] > [証明書の管理 (Certificate Management)] > [CSR のダウンロード (Download CSR)] を選択します。
 - [証明書の名前 (Certificate Name)] ドロップダウンリストで、[tomcat] を選択します。

- c) [CSR のダウンロード (Download CSR)] をクリックします。
- ステップ 3** CSR を使用して、認証局から署名付きアプリケーション証明書と CA ルート証明書を取得します。
- ステップ 4** 証明書を受け取ったら、[セキュリティ (Security)][証明書の管理 (Certificate Management)]>[証明書のアップロード (Upload Certificate)] を選択します。
- ステップ 5** ルート証明書をアップロードします。
- a) [証明書の名前 (Certificate Name)] ドロップダウンリストから、[tomcat-trust] を選択します。
- b) [ファイルのアップロード (Upload File)] フィールドで、[参照 (Browse)] をクリックして、ルート証明書ファイルを参照してください。
- c) [ファイルのアップロード (Upload File)] をクリックします。
- ステップ 6** アプリケーション証明書をアップロードします。
- a) [証明書の名前 (Certificate Name)] ドロップダウンリストで、[tomcat] を選択します。
- b) [ルート証明書 (Root Certificate)] フィールドに、CA ルート証明書の名前を入力します。
- c) [ファイルのアップロード (Upload File)] フィールドで、[参照 (Browse)] をクリックして、アプリケーションの証明書ファイルを参照してください。
- d) [ファイルのアップロード (Upload File)] をクリックします。
- ステップ 7** アップロードが完了したら、プライマリ Finesse サーバの CLI にアクセスします。
- ステップ 8** **utils service restart Cisco Finesse Notification Service** コマンドを入力して、Cisco Finesse Notification サービスを再起動します。
- ステップ 9** コマンド **utils service restart Cisco Tomcat** を入力して、Cisco Tomcat サービスを再起動します。
- ステップ 10** ルート証明書とアプリケーション証明書を Cisco Unified Intelligence Center パブリッシャ サーバにアップロードします。
- ステップ 11** アップロードが完了したら、Cisco Unified Intelligence Center サーバの CLI にアクセスします。
- ステップ 12** **utils service restart Intelligence Center Openfire Service** コマンドを入力して、Intelligence Center Openfire サービスを再起動します。
- ステップ 13** **utils service restart Intelligence Center Reporting Service** コマンドを入力して、Intelligence Center Reporting サービスを再起動します。

内部的な証明書の作成

Microsoft Certificate Server のセットアップ

この手順では、展開に Windows Server 2008 Active Directory サーバが使用されていることを前提とします。Windows 2008 ドメインコントローラの Active Directory 証明書サービスの役割を追加するには、次の手順を実行します。

手順

-
- ステップ 1 [スタート (Start)] をクリックし、[コンピュータ (Computer)] を右クリックして、[管理 (Manage)] を選択します。
 - ステップ 2 左側のペインで、[役割 (Roles)] をクリックします。
 - ステップ 3 右側のペインで、[役割の追加 (Add Roles)] をクリックします。
[役割の追加 (Add Roles)] ウィザードが開きます。
 - ステップ 4 [サーバの役割の選択 (Select Server Roles)] 画面で、[Active Directory 証明書サービス (Active Directory Certificate Services)] チェックボックスをオンにして [次へ (Next)] を選択します。
 - ステップ 5 [Active Directory 証明書サービスについて (Introduction to Active Directory Certificate Services)] 画面で、[次へ (Next)] をクリックします。
 - ステップ 6 [役割サービスの選択 (Select Role Services)] 画面で、[認証局 (Certification Authority)] チェックボックスをオンにして、[次へ (Next)] をクリックします。
 - ステップ 7 [セットアップの種類指定 (Specify Setup Type)] 画面で、[エンタープライズ (Enterprise)] を選択し、[次へ (Next)] をクリックします。
 - ステップ 8 [CA の種類指定 (Specify CA Type)] 画面で、[ルート CA (Root CA)] を選択し、[次へ (Next)] をクリックします。
 - ステップ 9 [公開キーのセットアップ (Set Up Private Key)]、[CA の暗号化を設定 (Configure Cryptography for CA)]、[CA 名を設定 (Configure CA Name)]、[有効期間を設定 (Set Validity Period)]、および [証明書データベースの設定 (Configure Certificate Database)] 画面で [次へ (Next)] をクリックして、デフォルトの値を受け入れます。
 - ステップ 10 [インストール時の選択を確認 (Confirm Installations Selections)] 画面で、情報を確認し、[インストール (Install)] をクリックします。
-

CA 証明書のダウンロード

この手順は、Windows 証明書サービスを使用していることを前提としています。次の手順を実行して、認証局からルート CA 証明書を取得します。ルート証明書を取得した後、各ユーザは Finesse にアクセスするために使用するブラウザにインストールする必要があります。

手順

-
- ステップ 1 Windows 2008 ドメイン コントローラで、CLI コマンド `ca.cert certutil - ca_name.cer` を実行します。
 - ステップ 2 ファイルを保存します。後で検索できるように、ファイルを保存した場所のメモを残しておきます。
-

Internet Explorer のルート証明書の導入

グループポリシーが Active Directory ドメインによって適用されている環境では、ルート証明書を各ユーザの Internet Explorer に自動的に追加できます。証明書を自動的に追加すると、設定に関するユーザ要求が簡略化されます。



- (注) 証明書の警告を回避するために、各ユーザは Finesse サーバの完全修飾ドメイン名 (FQDN) を使用してデスクトップにアクセスする必要があります。

手順

- ステップ 1 Windows 2008 ドメインコントローラで、[スタート (Start)] > [管理ツール (Administrative Tools)] > [グループポリシーの管理 (Group Policy Management)] をクリックします。
- ステップ 2 [デフォルトのドメインポリシー (Default Domain Policy)] を右クリックし、[編集 (Edit)] を選択します。
- ステップ 3 [グループポリシー管理コンソール (Group Policy Management Console)] で、[コンピュータ設定 (Computer Configuration)] > [ポリシー (Policies)] > [ウィンドウの設定 (Window Settings)] > [セキュリティ設定 (Security Settings)] > [公開キーポリシー (Public Key Policies)] に進みます。
- ステップ 4 [信頼されたルート証明機関 (Trusted Root Certification Authorities)] を右クリックし、[インポート (Import)] を選択します。
- ステップ 5 ca_name.cer ファイルをインポートします。
- ステップ 6 [コンピュータ設定 (Computer Configuration)] > [ポリシー (Policies)] > [Windows 設定 (Windows Settings)] > [セキュリティ設定 (Security Settings)] > [公開キーポリシー (Public Key Policies)] > [証明書サービス クライアント - 自動登録 (Certificate Services Client - Auto-Enrollment)] に進みます。
- ステップ 7 [設定モデル (Configuration Model)] リストから、[有効 (Enabled)] を選択します。
- ステップ 8 ドメインに含まれるコンピュータにユーザとしてサインインし、Internet Explorer を開きます。
- ステップ 9 ユーザが証明書を持っていない場合は、ユーザのコンピュータ上で `gpupdate.exe/target:computer /force` コマンドを実行します。

Internet Explorer ブラウザの証明書のセットアップ

CA 証明書を取得してアップロードした後、すべてのユーザが証明書を受け入れるか、証明書がグループポリシーによって自動的にインストールされる必要があります。

ユーザがドメインに直接ログインしていないか、グループポリシーが使用されていない環境では、証明書を受け入れたら、システム内の Internet Explorer のすべてのユーザが次の手順を実行する必要があります。

手順

- ステップ 1** Windows Explorer で、ca_name.cer ファイルをダブルクリックし、[開く (Open)] をクリックします。
- ステップ 2** [Install Certificate] > [Next] > [Place all certificates in the following store] をクリックします。
- ステップ 3** [参照 (Browse)] をクリックし、[信頼されたルート証明機関 (Trusted Root Certification Authorities)] を選択します。
- ステップ 4** [OK] をクリックします。
- ステップ 5** [次へ (Next)] をクリックします。
- ステップ 6** [終了 (Finish)] をクリックします。
認証局 (CA) から証明書をインストールしようとしていることを示すメッセージが表示されます。
- ステップ 7** [はい (Yes)] をクリックします。
インポートが正常に実行されたことを示すメッセージが表示されます。
- ステップ 8** 証明書がインストールされたことを確認するには、Internet Explorer を開きます。ブラウザのメニューから、[ツール (Tools)] > [インターネットオプション (Internet Options)] を選択します。
- ステップ 9** [コンテンツ (Content)] タブをクリックします。
- ステップ 10** [証明書 (Certificates)] をクリックします。
- ステップ 11** [信頼されたルート証明機関 (Trusted Root Certification Authorities)] タブをクリックします。
- ステップ 12** 新しい証明書がリストに表示されていることを確認します。
-

Firefox ブラウザの証明書のセットアップ

システム上の Firefox のすべてのユーザは、次の手順を一度実行して、証明書を受け入れる必要があります。



- (注) 証明書の警告を回避するために、各ユーザは Finesse サーバの完全修飾ドメイン名 (FQDN) を使用してデスクトップにアクセスする必要があります。
-

手順

- ステップ 1 Firefox のブラウザ メニューの [オプション (Options)] を選択します。
 - ステップ 2 [詳細設定 (Advanced)] をクリックします。
 - ステップ 3 [証明書 (Certificates)] タブをクリックします。
 - ステップ 4 [証明書を表示 (View Certificate)] をクリックします。
 - ステップ 5 [インポート (Import)] をクリックして、ca_name.cer ファイルを参照します。
-



索引

A

- Active Directory [188](#)
 - スーパーバイザ [188](#)
 - 設定 [188](#)
- AW データ ベース [122](#)

C

- CCE コール サーバ [44, 76](#)
 - VM [76](#)
 - ゴールデン テンプレート [44](#)
- CCE データ サーバ [44, 76](#)
 - VM [76](#)
 - ゴールデン テンプレート [44](#)
- Cisco Contact Center ソフトウェア [7](#)
- Cisco Unified OS Administration [214](#)
 - およびアップグレード [214](#)
- CVP Reporting Server [99](#)
 - インストール [99](#)

D

- DNS 設定 [87](#)

F

- Finesse [47](#)
 - ゴールデン テンプレート [47](#)
- Finesse セカンダリ [79](#)
 - VM [79](#)
- Finesse プライマリ [105](#)
 - インストール [105](#)

I

- ICMDBA [120](#)
- ISO ファイル [83](#)
 - マウント [83](#)
 - マウントおよびアンマウント [83](#)

M

- Microsoft SQL Server [93](#)
 - インストール [93](#)
- Microsoft Windows Server [89](#)
 - インストール [89](#)
- Microsoft ソフトウェア [8](#)

O

- OVA ファイル [83](#)

P

- PowerCLI [49](#)

Q

- QoS [40](#)

S

- SNMP [229](#)

U

- Unified Communications Manager [47](#)
 - ゴールデンテンプレート [47](#)
- Unified Communications Manager サブスクライバ [78](#)
 - VM [78](#)
- Unified Communications Manager パブリッシャ [78, 105](#)
 - VM [78](#)
 - インストール [105](#)
- Unified CVP コール/VXML サーバ [44](#)
 - ゴールデンテンプレート [44](#)
- Unified CVP サーバ [45, 46, 77](#)
 - ゴールデンテンプレート [45, 46, 77](#)
- Unified CVP レポートニング ユーザ [188](#)
 - Unified IC の認証 [188](#)
- Unified CVP レポート テンプレート [188](#)
 - 取得 [188](#)
- Unified Intelligence Center [47, 71, 189](#)
 - ゴールデンテンプレート [47](#)
 - データ ソース [189](#)
 - ライセンス [71](#)
- Unified Intelligence Center サブスクライバ [80](#)
 - VM [80](#)
- Unified Intelligence Center パブリッシャ [80, 105](#)
 - VM [80](#)
 - インストール [105](#)

V

- VMWare ツール [91](#)
- vSphere [25](#)

W

- WinImage [49](#)

あ

- アップグレード [214](#)
 - およびバックアップ [214](#)
 - の長さ [214](#)
- アップグレードファイル [215](#)
 - アクセス [215](#)
- 宛先サーバ、VM が存在する [4](#)
- アンチウイルス [8](#)
- アンチウイルス ソフトウェア [88](#)

い

- インストール [88, 89, 91, 93, 99, 105, 229](#)
 - CVP Reporting Server [99](#)
 - Finesse プライマリ [105](#)
 - Microsoft SQL Server [93](#)
 - Microsoft Windows Server [89](#)
 - Unified Communications Manager パブリッシャ [105](#)
 - Unified Intelligence Center [105](#)
 - VMWare ツール [91](#)
 - アンチウイルス ソフトウェア [88](#)
 - 言語パック [229](#)

か

- 外部 AW-HDS-DDS [104](#)
- 仮想マシン [4, 76, 78, 79, 80](#)
 - CCE コール サーバ [76](#)
 - CCE データ サーバ [76](#)
 - Finesse セカンダリ [79](#)
 - Unified Communications Manager サブスクライバ [78](#)
 - Unified Communications Manager パブリッシャ [78](#)
 - Unified Intelligence Center サブスクライバ [80](#)
 - Unified Intelligence Center パブリッシャ [80](#)
 - 宛先サーバ上 [4](#)

き

- 基本設定 [6, 119, 120](#)

け

- 言語パック [229](#)

こ

- ゴールデンテンプレート [42, 44, 45, 46, 47, 77](#)
 - CCE コール サーバ [44](#)
 - CCE データ サーバ [44](#)
 - Finesse [47](#)
 - Unified Communications Manager [47](#)
 - Unified CVP コール/VXML サーバ [44](#)
 - Unified CVP サーバ [45, 46, 77](#)
 - Unified Intelligence Center [47](#)
- コミュニティ ストリング [229](#)

さ

サーバ [5](#)

し

自動化 [49, 52, 58](#)

zip ファイル [49](#)

エラー [52, 58](#)

ステータス レポート [52, 58](#)

ソフトウェア [49](#)

自動化スプレッドシート [50, 53](#)

照合順序 [93, 96](#)

せ

設定ソフトウェア [6](#)

そ

ソフトウェア [7, 8, 10](#)

Microsoft [8](#)

アンチウイルス [8](#)

ブラウザ [10](#)

ソフトウェア、設定 [6](#)

ソリューションのコンポーネント [4](#)

た

タイムゾーン [189](#)

データ ソース [189](#)

ち

直接インストール [42](#)

関連項目 : [install](#)

つ

追加 [189](#)

データ ソース [189](#)

通知宛先 [229](#)

て

データ サーバ [122](#)

AW データベース [122](#)

データ ソース [189](#)

追加 [189](#)

ね

ネットワーク設計 [25](#)

は

パーティション [214](#)

アクティブおよび非アクティブ [214](#)

ふ

ブラウザのソフトウェア [10](#)

へ

ベスト プラクティス [71](#)

ライセンス [71](#)

よ

の要件 [49](#)

ソフトウェア [49](#)

要件 [7](#)

ソフトウェア [7](#)

ら

ライセンス [71](#)

取得 [71](#)

ベスト プラクティス [71](#)

れ

レジストリ設定 [66](#)

レポートテンプレート **188**
 アクセス **188**

ろ

ローカリゼーション **96, 229**
ロガー データベース **117**
ログイン **188**
 スーパーバイザ **188**