Cisco CloudCenter リリース 4.8.x インストール ガイド

初回更新日:2017年7月19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/

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。シスコとこれら各社は、商品性の保証、特定目的への準拠の保証と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)

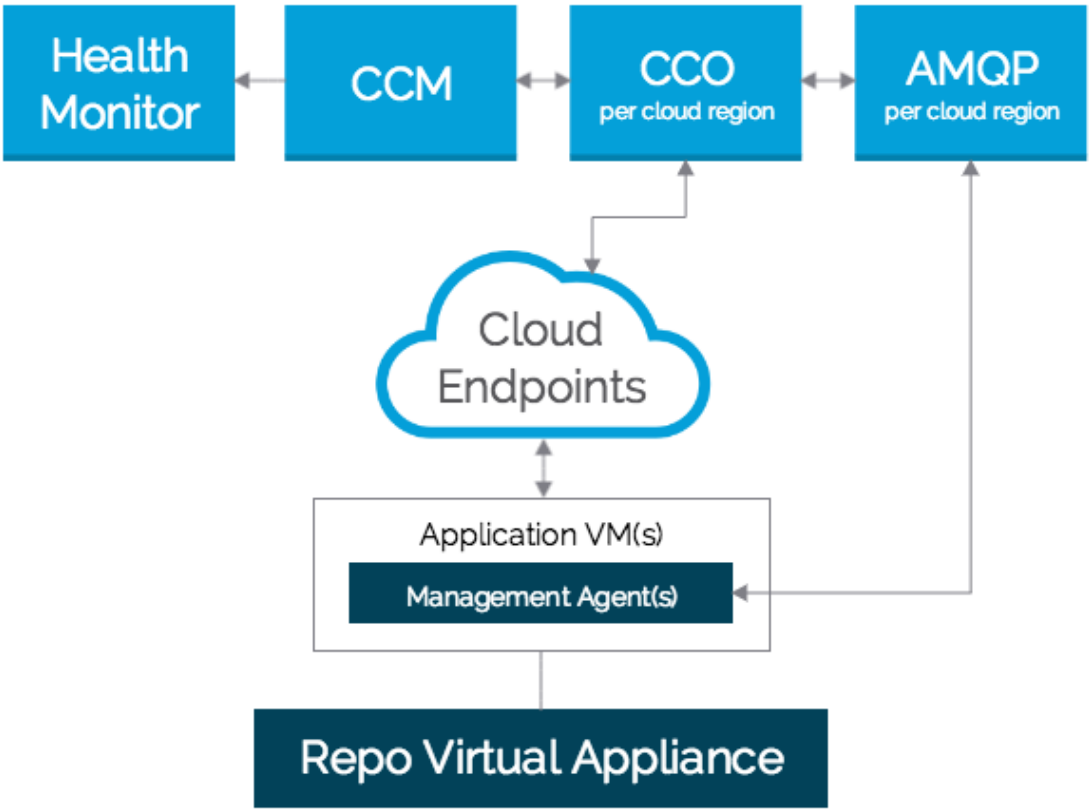
© 2017 Cisco Systems, Inc. All rights reserved.

1. 仮想アプライアンスの概要 2
2. 高可用性のベスト プラクティス 7
3. インストール方法 10
4. フェーズ 1: インフラストラクチャの準備 13
4.1 ハードウェア要件 13
4.2 クラウドの微妙な違い 14
4.3 仮想アプライアンスのプロセス 18
4.4 前提条件チェッカー JSON ファイル 30
5. フェーズ 2: ファイアウォール ルールの設定 34
5.1 ファイアウォール ルールの概要 34
5.2 CCM ファイアウォール ルール 35
5.3 CCO ファイアウォール ルール 38
5.4 AMQP ファイアウォール ルール 39
5.5 モニタ ファイアウォール ルール 40
5.6 リポジトリ ファイアウォール ルール 40
6. フェーズ 3: 前提条件チェッカーの実行 40
7. フェーズ 4: コンポーネントの設定 42
7.1 フェーズ 4 の概要 42
7.2 CCM（必須） 43
7.3 モニタ（必須） 60
7.4 リポジトリ（条件付き） 60
7.5 クラウド リージョンごと（必須） 62
7.6 ワーカー（条件付き） 75
8. CloudCenter の設定 76
8.1 管理者アカウントの設定 76
8.2 クラウドの設定 80
8.3 CCM への CCO の登録 161
8.4 イメージ マッピング 163
8.5 インスタンス タイプの管理 165
8.6 クラウド ストレージの設定 167
8.7 イメージ ID の設定 170
9. インストールに関する FAQ 177

仮想アプライアンスの概要

- CloudCenter アプライアンス アーキテクチャ
- 仮想アプライアンス ファイル
- モード
- ネットワーク アーキテクチャ図
- コンポーネント
  - CloudCenter の展開ごと
  - クラウド リージョンごと
- CloudCenter 展開の想定 VM 数

CloudCenter アプライアンス アーキテクチャ



仮想アプライアンス ファイル

CloudCenter コンポーネントをインストールする最も簡単な方法は、仮想アプライアンスの方法を使用することです。事前にパッケージ化されたシスコ認定の仮想アプライアンスを使用できるため、CloudCenter の顧客の大半は仮想アプライアンスを使用して CloudCenter のすべてのコンポーネントをセットアップします。

各 CloudCenter コンポーネントの**仮想アプライアンス**は、software.cisco.com から利用可能です。手順については、README ファイルを参照してください。

> ⚠ クラウドごとのサポートされるコンポーネントの完全なリストについては、「Virtual Appliances」を参照してください。

独自のベース オペレーティング システム イメージと **CloudCenter インストーラ**を使用して **CloudCenter を手動でインストール**するには、CloudCenter サポート チームに問い合わせ、手動のインストーラの説明を入手してください。

モード

拡張性と高可用性の要件に基づいて、さまざまなモードの CloudCenter のコンポーネントを設定できます。各モードには固有のインフラストラクチャ要件（VM、ロード バランサ（LB）、仮想/Elastic IP アドレス）があります。各種の CloudCenter コンポーネントは、同じ導入において異なるモードで設定できます。たとえば、CCM を HA モードで、AMQP を非 HA モードで設定できます。

各モードのネットワーク アーキテクチャの図の例は、このセクションの終わりにあります。

- 非 HA：このモードはすべてのコンポーネントに対して利用可能です。同じ VM 上に CCM の Web サーバとデータベースの両方があるとき、各コンポーネントには 1 つの VM が必要です。
- 非 HA スタンドアロン：このモードは CCM Web サーバに対してのみ利用可能です。2 つの別個の VM 上に CCM の Web サーバとデータベースがあるとき、各コンポーネントには 1 つの VM が必要です。*これは、将来的に HA モードに移行する場合に推奨されるモードです。*
- HA：このモードは、CCM、PostgreSQL データベース、CCO、および AMQP サーバに対してのみ利用可能です。
  - 次のコンポーネントには別個の 2 つの VM が必要です。
    - CCM Web サーバ（2）とロード バランサ
    - PostgreSQL データベース（2）とロード バランサ
    - AMQP（2）とロード バランサ
  - CCO（3）とロード バランサの場合、3 つの別個の VM が必要です。
  - クラウド ヘルス モニタ（1）の 1 つの VM - 必要なコンポーネント。

各モードに必要なサーバ数の詳細な明細については、このページの最後の表を参照してください。

ネットワーク アーキテクチャ図

コンポーネント

CloudCenter プラットフォームは 4 つの必要なコンポーネントと複数のオプション コンポーネントで構成されます。各コンポーネント VM は、各コンポーネントを設定した*モード*（非 HA、非 HA スタンドアロン、または HA）に基づいて***ロール***が割り当てられます。次に例を示します。

- 非 HA 展開の *CCM* のロール
- 非 HA スタンドアロン展開の *CCM_SA* と MGMTPOSTGRES のロール
- HA 展開の CCM_SA_PRIMARY、CCM_SA_SECONDARY、MGMTPOSTGRES_MASTER、MGMTPOSTGRES_SLAVE、CCM_LB のロール

各コンポーネントおよびモードの***ロール***は以下のセクションで説明しています。

CloudCenter の展開ごと

これらのコンポーネントは展開ごとに設定します。

CCM（必須）

CloudCenter Manager（CCM）は、ユーザがさまざまなクラウド上のワークロードのモデル化、展開、および管理を行うことができる、一元化された管理コンソールです。

CCM は、各 CloudCenter Orchestrator（CCO）と直接やり取りしてクラウド環境を管理します。ユーザは、CCM UI または REST API を使用して CloudCenter の機能にアクセスできます。

CCM モード	役割名	タイプ（Type）	目的
非 HA	CCM	VM	CCM Web サーバとデータベース
非 HA スタンドアロン	CCM_SA	VM	非 HA スタンドアロン CCM – Web サーバのみ
非 HA スタンドアロン	MGMTPOSTGRES	VM	非 HA スタンドアロン PostgreSQL データベース サーバのみ
HA	CCM_SA_PRIMARY	VM	非 HA スタンドアロン プライマリ CCM – Web サーバのみ
HA	CCM_SA_SECONDARY	VM	非 HA スタンドアロン セカンダリ CCM – Web サーバのみ
HA	MGMTPOSTGRES_MASTER	VM	PostgreSQL のマスター データベース サーバ
HA	MGMTPOSTGRES_SLAVE	VM	PostgreSQL スレーブ データベース サーバ
HA	CCM_LB	ロード バランサ	両方の CCM VM 間での着信要求のバランス
HA	MGMTPOSTGRES_VIP	仮想 IP（VIP）または Elastic IP（EIP）	いずれかのサーバがダウンすると、アクティブ サーバへの動的なスイッチングを有効にするように、PostgreSQL サーバの 1 つに接続します

クラウド ヘルス モニタ（必須）

クラウド ヘルス モニタ（モニタ）は、クラウドと CCO のヘルス ステータスを監視する必須の独立型 CloudCenter コンポーネントです。モニタでは次の処理が実行されます。

- クラウドごとに CCO のヘルス ステータスを定期的にチェックする。
- クラウドのヘルス ステータス変更イベントを保持する。
- CCM UI のダッシュボードにこれらのチェック結果を表示する。
- CCM ログと CCO ログのログ リポジトリを含める。

Elasticsearch、Logstash、Kibana は ELK スタックと総称され、ヘルス モニタをインストールするとデフォルトでインストールされます。

モニタ モード	役割	タイプ（Type）	目的
非 HA	MON	VM	クラウド リージョンのヘルスを監視し、CCM に報告します

リポジトリ仮想アプライアンス

リポジトリ仮想アプライアンスには、複数のソフトウェア パッケージと、CloudCenter パッケージが使用するより小さなコンポーネント（サービス バンドル、ソフトウェア パッケージ、バイナリ、スクリプト、Docker イメージなど）の仮想アプライアンスが含まれます。リポジトリ仮想アプライアンスをインストールして設定すると、含まれるコンポーネントがインストールされ、関連付けられているプロパティは、CCM ウィザード、CCO ウィザード、または AMQP ウィザードで必要な場合に設定できます。

このリポジトリ アプライアンス：

- CentOS7 サーバ上で Nginx を使用します。
- CloudCenter の各リリースに固有のバージョンです。

リポジトリ モード	役割	タイプ（Type）	目的
非 HA	REPO	VM	サービス バンドル、パッケージ ストア、スクリプトなどのため

クラウド リージョンごと

*クラウド リージョン*とは、CloudCenter でサポートされる単一のパブリック クラウド リージョン、仮想化されたプライベート データセンター、またはプライベート クラウドのことです。各クラウド リージョンは、クラウドの設定時に CCM UI で特定されます。CloudCenter プラットフォームで管理する必要がある*クラウド リージョン*ごとに、以下の CloudCenter コンポーネントをセットアップして設定する必要があります。

CCO（必須）

CloudCenter Orchestrator（CCO）は、すべてのクラウド リージョンに展開する必要があります。CCO は、アプリケーションの導入およびランタイム管理を処理するためにクラウド エンドポイントとインテリジェントに対話するバックエンド サーバです。CCO は、クラウド導入時の複雑さを軽減するため、アプリケーションを基盤となるクラウド インフラストラクチャから切り離します。

- アプリケーション ネットワークが完全に分離されており、かつ**発信接続がない**場合を除き、CloudCenter ではクラウド リージョンごとに 1 つの CCO が必要です。
- CloudCenter は、個別の CCO を必要とする**プライベート クラウドとして VPN で分離されたネットワーク（VPC）**を処理します。
- 各 CCO を CCM に登録する必要があります。CCO が展開されているクラウドに関係なく、CCO は CCM と直接通信します。

クラウド リージョンごとの CCO

クラウド タイプに応じて、クラウド リージョンまたはプライベート データセンターごとに 1 つの CCO が必要です。

クラウド タイプ	CCO ごとに、以下の 1 つの組み合わせのみサポート	CCO ごとに、以下を任意の数だけサポート
AWS	地域	• アカウント • サブアカウント • アイデンティティとアクセス管理（IAM）

VMware vCenter	vCenter インスタンス	• データセンター • クラスタ（Clusters） • リソース プール • アカウント • データ ストア • データストア クラスタ
VMware vCD	vCD インスタンス/エンドポイント	vCD
Microsoft Azure	地域	• ネットワーク • クラウド サービス • アカウント
Google Cloud	地域	• プロジェクト • アカウント
OpenStack	地域	• テナント • ネットワーク • アカウント
SoftLayer（Bluemix）	地域	• アカウント • ネットワーク
Alibaba	地域	• アカウント • ネットワーク
Dimension Data（DiData）	地域	• アカウント • ネットワーク
Cisco UCSD	UCSD インスタンス	N/A

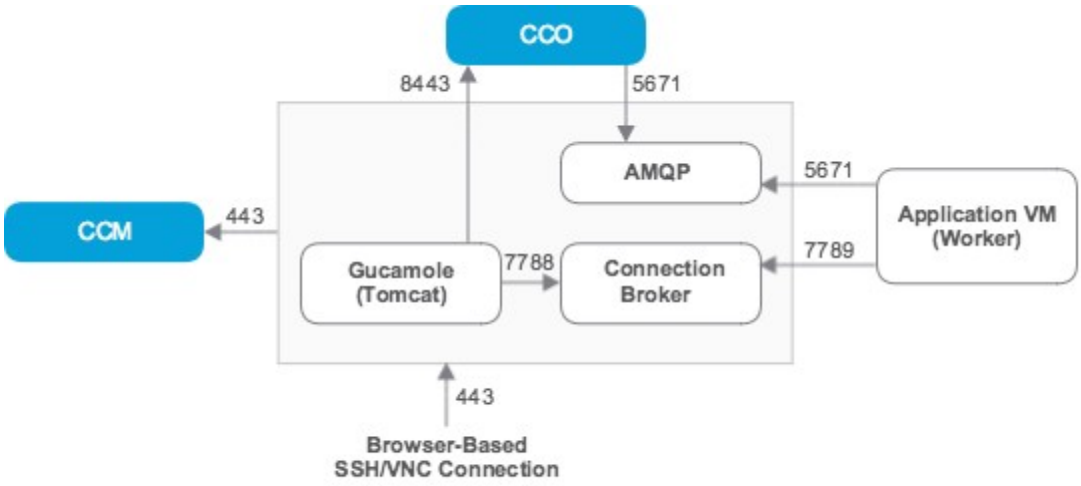
CCO モード	役割	タイプ（Type）	目的
非 HA	CCO	VM	オーケストレータ
HA	CCO_PRIMARY	VM	プライマリ オーケストレータ
HA	CCO_SECONDARY	VM	セカンダリ オーケストレータ
HA	CCO_TERTIARY	VM	ターシャリ オーケストレータ
HA	CCO_LB	ロード バランサ	両方の CCO VM 間での着信要求のバランス

AMQP（必須）

CloudCenter プラットフォームは、Advanced Message Queuing Protocol（AMQP）に基づく CCO とエージェント VM 間の通信を特徴としています。CloudCenter プラットフォームは、AMQP 実装のオープン ソース メッセージ ブローカとして RabbitMQ を採用しています。

> 分離されたネットワーク（Amazon の VPC など）でアプリケーション VM を実行する場合は、VM が RabbitMQ に接続できるように、発信トラフィックのみに NAT 規則を設定します。

次の図に、CloudCenter コンポーネントと AMQP の関係を示します。CCO の実装ごとに 1 つの AMQP インスタンスが必要になることに注意してください。



AMQP モード	役割	タイプ(Type)	目的
非 HA	AMQP	VM	RabbitMQ ベースのメッセージ キュー
HA	AMQP_PRIMARY	VM	プライマリ RabbitMQ ベースのメッセージ キュー
HA	AMQP_SECONDARY	VM	セカンダリ RabbitMQ ベースのメッセージ キュー
HA	AMQP_LB	ロード バランサ	両方の AMQP VM 間での着信メッセージのバランス

ベース OS イメージの準備(動的ブートストラップをサポートしていないクラウドの場合は必須)

ベース OS イメージ(ワーカー イメージとも呼びます)は、動的ブートストラップをサポートしていないクラウドの場合にのみ必要になります。動的ブートストラップをサポートしていない一部のクラウド(VMware、SoftLayer、DiData など)では、ベース OS イメージの準備が必要になります。CloudCenter ソフトウェアは、CentOS6 用の仮想アプライアンスを提供します。詳細については、「Base OS Images」を参照してください。

ベース OS タイプ	役割	目的
VM イメージ	LINUX_WORKER_*OS_VERSION*	アプリケーションのオーケストレーション中に VM を起動するときに使用するマシン イメージ。
VM イメージ	WINDOWS_WORKER_*OS_VERSION*	アプリケーションのオーケストレーション中に VM を起動するために使用するマシン イメージ。

CloudCenter 展開の想定 VM 数

クラウド リージョン 1 つの基本展開では、通常、次の VM が必要です。

必要なコンポーネント	非 HA	非 HA スタンドアロン	HA	注記(Notes)
CCM	1 VM	1 VM	2 VM	CCM UI へのアクセス
MGMTPOSTGRES	-	1 VM	2 VM	CCM データベース
CCM LB	-	-	1 VM	HA モードの LB
CCO	1 VM	1 VM	3 VM	クラウド リージョンごとに 3 VM
CCO LB	-	-	1 VM	HA モードの LB – クラウド リージョンごとに 1 VM
AMQP	1 VM	1 VM	2 VM	クラウド リージョンごと
AMQP LB	-	-	1 VM	HA モードの LB
Monitor	1 VM	1 VM	1 VM	ログに必要
合計	**4 VM**	**5 VM**	**13 VM**	**一般的な基本展開**

クラウド リージョン 2 つの基本展開では、通常、次の VM が必要です。

必要なコンポーネント	非 HA	非 HA スタンドアロン	HA	注記（Notes）
CCM	1 VM	1 VM	2 VM	CCM UI へのアクセス
MGMTPOSTGRES	-	1 VM	2 VM	CCM データベース
CCM LB	-	-	1 VM	HA モードの LB
CCO	2 VM	2 VM	6 VM	HA モードではクラウド リージョンごとに 3 VM
CCO LB	-	-	2 VM	HA モードの LB – クラウド リージョンごとに 1 VM
AMQP	2 VM	2 VM	4 VM	クラウド リージョンごと
AMQP LB	-	-	2 VM	HA モードの LB
Monitor	1 VM	1 VM	1 VM	ログに必要
合計	**6 VM**	**7 VM**	**20 VM**	**一般的な基本展開**

高可用性のベスト プラクティス

- 概要
- CloudCenter 展開の想定 VM 数
- すべてのコンポーネントの一般的な要件
- ロード バランサの要件
- CCM データベース HA
- CCM HA
- CCO HA
- AMQP HA

概要

典型的な高可用性（HA）ネットワークは、HA 仮想アプライアンス アーキテクチャに示しています。

クラウド リージョン 1 つの *CloudCenter 展開の想定 VM 数*を確認するには、「仮想アプライアンスの概要」を参照してください。

CloudCenter 展開の想定 VM 数

クラウド リージョン 1 つの基本展開では、通常、次の VM が必要です。

必要なコンポーネント	非 HA	非 HA スタンドアロン	HA	注記（Notes）
CCM	1 VM	1 VM	2 VM	CCM UI へのアクセス
MGMTPOSTGRES	-	1 VM	2 VM	CCM データベース
CCM LB	-	-	1 VM	HA モードの LB
CCO	1 VM	1 VM	3 VM	クラウド リージョンごとに 3 VM
CCO LB	-	-	1 VM	HA モードの LB – クラウド リージョンごとに 1 VM
AMQP	1 VM	1 VM	2 VM	クラウド リージョンごと
AMQP LB	-	-	1 VM	HA モードの LB
Monitor	1 VM	1 VM	1 VM	ログに必要
合計	**4 VM**	**5 VM**	**13 VM**	**一般的な基本展開**

クラウド リージョン 2 つの基本展開では、通常、次の VM が必要です。

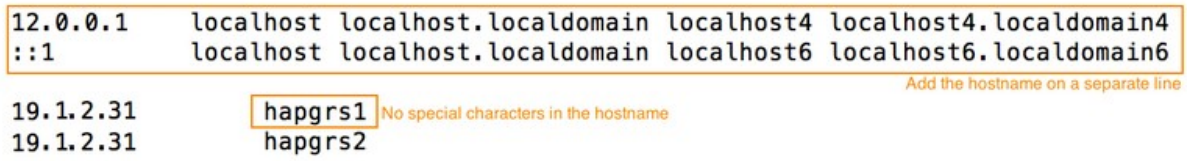
必要なコンポーネント	非 HA	非 HA スタンドアロン	HA	注記（Notes）
CCM	1 VM	1 VM	2 VM	CCM UI へのアクセス
MGMTPOSTGRES	-	1 VM	2 VM	CCM データベース
CCM LB	-	-	1 VM	HA モードの LB
CCO	2 VM	2 VM	6 VM	HA モードではクラウド リージョンごとに 3 VM
CCO LB	-	-	2 VM	HA モードの LB – クラウド リージョンごとに 1 VM

AMQP	2 VM	2 VM	4 VM	クラウド リージョンごと
AMQP LB	-	-	2 VM	HA モードの LB
Monitor	1 VM	1 VM	1 VM	ログに必要
合計	**6 VM**	**7 VM**	**20 VM**	**一般的な基本展開**

すべてのコンポーネントの一般的な要件

HA モードでインストールされている CloudCenter コンポーネントは、次の要件に従う必要があります。

- シングル ポイント障害を避けるためには、独立したゾーンまたはリージョンに、各コンポーネントの高可用性 VM をセットアップします。
- ローカルホストを指定し、**/etc/hosts** ファイルで*ホストのホスト名が解決可能な状態*にします。
  - **ローカルホスト**：次の例では、*127.0.0.1* およびコンポーネント（**/etc/hosts** ファイル内の *hapgrs1* および *hapgr s2*）の IP アドレスにローカルホストを追加します。



  - **ホスト名**：
    - 認証が失敗する原因となるため、データベース サーバにアンダースコア、ハイフン、スペースを含む特殊文字を含めることはできません。
    - **VM のインストールおよび設定後にホスト名を変更すると、未知の問題を引き起こす可能性があります。**
    - ホスト名をローカルホストと同じ行にすることはできません。**/etc/hosts** ファイル内の別の行にホスト名を追加します。

ロード バランサの要件

ベスト プラクティスとして、真の HA サポートを提供するためには HA モードでコンポーネントごとに 1 つのロード バランサを設定することをお勧めします。

- CCM VM
- CCO VM
- AMQP VM

各コンポーネントにロード バランサを設定するときは、次のようにします。

- HA モードのコンポーネント（CCM、CCO、または AMQP コンポーネント）ごとに VM の 1 つにトラフィックを送信します。
- リスナーには TCP プロトコルを使用します。たとえば、TCP を使用して証明書交換の手順が透過的になるように汎用のロード バランサ アプリケーションを設定できます。
- CCM、CCO、AMQP ロード バランサ間の通信には SSL 証明書を使用します。
- セッション スティッキ性ポリシーを有効にします。詳細については、ロード バランサのドキュメントを参照してください。
- CCM UI から CCO IP フィールドを設定するときは、ロード バランサの IP アドレスを使用します。
- 非 HA モードから HA モードにコンポーネントをアップグレードする場合、既存の展開に新しい VM を追加することがあります。この場合、以前設定したコンポーネント IP アドレスは、このコンポーネントのロード バランサの IP アドレスに置き換えます。

CCM データベース HA

CCM サーバを設定する前にデータベース サーバを設定します。CCM サーバは、セットアップされ実行中のデータベース サーバに依存します。

CCM データベースは PostgreSQL タイプを使用し、ドキュメントで MGMTPOSTGRES のロールとして識別されます。2 つの データベース サーバが連携して動作し、マスター サーバに障害が発生しても 2 番目のサーバが迅速に引き継ぐことができます。

CCM データベース HA を設定するには、次のサーバをインストールする必要があります。MGMTPOSTGRES_MASTER：

- データを変更し、負荷を伝送するサーバ。
- MGMTPOSTGRES_SLAVE：マスター サーバでの変更に対し、応答またはレプリケーションを行うサーバ。
- 仮想 IP（VIP）：クラウドで起動された PostgreSQL インスタンスは、クラウド管理者が設定した VIP を使用して企業のネットワーク ルーティングを処理できる必要があります。

その他の微妙な違い：

- 同じクラウドやデータセンターに 2 つのデータベース サーバを 2 つの CCM サーバとして配置します。これにより、次のようになります。
  - マスター/スレーブ HA セットアップにより、プライマリ サーバに障害が発生した場合にセカンダリ サーバがシームレスに引き継ぐことができます。

    - 障害が発生したサーバがオンラインに戻ると、新しいマスター サーバからデータが自動的に同期されます。オフラインになっていたサーバがスレーブ サーバになります。古いマスター サーバがオンラインに戻ると、クラスタに再参加し、自動的に新しいスレーブ サーバになります。
- 該当する MGMTPOSTGRES インスタンスに仮想 IP 設定を正確にルーティングすることを確認します。
- セカンダリ CCM サーバで sudo 権限がない場合、プライマリ CCM から CCM ウィザードの Configure_HA フィールドが実行されても、セカンダリ CCM サーバ上の Tomcat Service は再起動しません。Tomcat Service をリモートで開始する必要がある場合は、セカンダリ CCM サーバで sudo 権限を設定します。

CCM HA

CloudCenter CCM とデータベース サーバは連携して次の HA ソリューションを提供します。

- 同期トランザクション：すべてのサーバがトランザクションを完了するまでコミット済みとは見なされません。
- フェールオーバー：フェールオーバーによってデータが失われないようにします。一方の CCM サーバがオフラインになると、もう一方のサーバがプライマリ サーバとして引き継がれ、必要なすべてのアクティビティが引き続き処理されます。
- 一貫性：両方のサーバのデータベースと設定の変更は同期されているため、両サーバに結果が返されます。

> CloudCenter は、クロス リージョンにおける CCM HA の設定をサポートしません。

CCM HA を設定するには、次のサーバをインストールする必要があります。

- 2 つの CCM サーバ：
    - CCM_SA_PRIMARY
    - CCM_SA_SECONDARY
- 1 つのロード バランサ：ロード バランサの背後で 2 つの CCM サーバが同時に実行されます。

その他の微妙な違い：

- CCM HA のインストールは、*AWS*、*OpenStack*、*および VMware* のクラウドでテストおよび検証されています。
- カスタム証明書を使用する場合はプライマリ CCM からのみ生成し、その他すべてのコンポーネント（たとえば、他の CCM、すべての CCO、AMQP、モニタなど）にコピーする必要があります。

CCO HA

各サーバはアクティブであり、クラスタ内のすべてのサーバはオーケストレーション タスクを並行して実行します。クラスタ内のいずれかのサーバがオフラインになっても、他のアクティブなサーバは引き続きオーケストレーション タスクを処理します。オフライン サーバがオンラインに戻ると、アクティブなサーバからデータが自動的に同期されます。

> CloudCenter は、クロス リージョンにおける CCO HA の設定をサポートしません。

CCO HA を設定するには、次のサーバをインストールする必要があります。

- 3 ノード MongoDB クラスタをサポートする 3 つの VM：
    - CCO_PRIMARY（CCO_PRIMARY で CCO 設定ウィザードを実行します。）CCO_SECONDARY
    - CCO_TERTIARY。
- 1 つのロード バランサ：ロード バランサの背後で 3 つの CCO サーバが同時に実行されます。

> HA モードで CCO を初めて設定するときは、各 CCO にロード バランサをポイントし、3 つの CCO のそれぞれを CCM に登録する必要があります。手順の詳細については、「CCM への CCO の登録」を参照してください。

AMQP HA

> CloudCenter は、クロス リージョンにおける AMQP HA の設定をサポートしません。

AMQP HA の設定を開始する***前の***前提条件：

- RabbitMQ クラスタの上にロード バランサを設定した後、AMQP サーバの IP アドレスを読み取るように CCO サーバを設定します。
- 上記の「*一般的な要件*」セクションで言及した /etc/hosts ファイルのホスト名の要件に加え、**両方**の AMQP サーバにすでに存在する /etc/hosts ファイル内のプライマリおよびセカンダリ AMQP インスタンスの**両方**に対してホスト名を追加する必要があります。

/etc/hosts ファイル

```
<amqp1_IPaddress> amqp1Hostname
<amqp2_IPaddress> amqp2Hostname
```

/etc フォルダ内にホスト名ファイルを追加し、次にサーバを再起動します。このステップは、HA モードで AMQP をインストールするために必須です。**両方**の AMQP サーバにすでに存在する /etc/hosts ファイル内のプライマリおよびセカンダリ AMQP インスタンスの**両方**に対してホスト名を追加する必要があります。

/etc/hostname ファイル /etc/hosts ファイル

```
vi /etc/hostname

#remove the existing name and add a custom AMQP hostname, save and exit file.
HOSTNAME <amqpHostname>

reboot

#verify that the reboot did not change the hostname.
```

AMQP HA を構成するには、次のサーバをインストールする必要があります。

- 2 つの AMQP サーバ:
  - AMQP_PRIMARY
  - AMQP_SECONDARY
- 1 つのロード バランサ:ロード バランサの背後で 2 つの AMQP サーバが同時に実行されます。

インストール方法

このページを印刷して必要な情報を書き込み、いつでも参照できるようにしてください。

アプローチ

CloudCenter プラットフォームをインストールするには、次のフェーズを完了する必要があります。

フェーズ	説明
1	**インフラストラクチャの準備** VM、ロード バランサ、仮想 IP(VIP)または Elastic IP(EIP)を起動および識別し、CloudCenter のコンポーネントをインストールして設定します。
2	**ネットワーク ルールの設定** さまざまなコンポーネント間の通信を可能にするネットワーク ルールを設定します。
3	**ネットワーク コンプライアンス チェックの実行** ネットワーク ルールが適切に設定されていることを確認するには、ネットワーク コンプライアンス チェックを実行します。

4	**コンポーネントの設定** 仮想マシンでインストーラを実行して、CloudCenter コンポーネントをインストールし、設定ウィザードを起動して、コンポーネントのプロパティを設定します。 1. CCM 設定（必須） • CCM 非 HA • CCM 非 HA スタンドアロン • CCM HA 2. クラウド リージョンごとの設定（必須） a. AMQP（必須） i. AMQP 非 HA ii. AMQP HA b. CCO（必須） i. CCO 非 HA ii. CCO HA 3. モニタ設定（必須） a. モニタ非 HA 4. リポジトリ（条件付き） 5. アプリケーション VM 用のカスタム Linux イメージ（ワーカー イメージ）- ワーカー（条件付き）

インストールの参照メモ（参照用に印刷）

CloudCenter プラットフォームのインストール時には、IP アドレスや DNS 名、その他のエントリを、後の使用のためにメモするよう頻繁に指示されます。この作業はインストール プロセスの一部です。相互参照やフォローアップのためにメモや参照を追跡するのに役立つよう、シスコでは次の表を用意しています。

追跡リスト	リンク	メモ
☐ 1	CCM（必須）	非 HA • メール（Mail） • SMTP ホスト（SMTP Host） • SMTP ポート（SMTP Port） • SMTP 認証（SMTP Auth） • Mail_User • メール ユーザ（Mail User） • パスワード（Password） • ユーザから（From User） • 表示名（Display Name） • Server_Info • パブリック DNS（Public DNS） • モニタ URL（Monitor URL） • Hazelcast IP • 外部 URL（External URL） • ネットワーク（Network） • ホストネーム（Hostname） • インターフェイス（Interface）
☐ 1	CCM（必須）	非 HA スタンドアロン • CCM IP • メール（Mail） • SMTP ホスト（SMTP Host） • SMTP ポート（SMTP Port） • SMTP 認証（SMTP Auth） • Mail_User • メール ユーザ（Mail User） • パスワード（Password） • ユーザから（From User） • 表示名（Display Name） • Server_Info • パブリック DNS（Public DNS） • モニタ URL（Monitor URL） • Hazelcast IP • 外部 URL（External URL） • ネットワーク（Network） • ホストネーム（Hostname） • インターフェイス（Interface）

☐ 1	CCM
	（必須）
		HA
		• マスター データベースのホスト名（Master database Hostname）
		• マスター データベースのプライベート IP（Master database Private IP）
		• スレーブ データベースのホスト名（Slave database Hostname）
		• スレーブ データベースのプライベート IP（Slave database Private IP）
		• VIP
		• プライマリ CCM IP
		• セカンダリ CCM ノード IP
		• メール（Mail）
		  • SMTP ホスト（SMTP Host）
		  • SMTP ポート（SMTP Port）
		  • SMTP 認証（SMTP Auth）
		• Mail_User
		  • メール ユーザ（Mail User）
		  • パスワード（Password）
		  • ユーザから（From User）
		  • 表示名（Display Name）
		• Server_Info
		  • パブリック DNS（Public DNS）
		  • モニタ URL（Monitor URL）
		  • Hazelcast IP
		  • 外部 URL（External URL）
		• ネットワーク（Network）
		  • ホストネーム（Hostname）
		  • インターフェイス（Interface）

☐ 2	クラウド リージョンごと （必須）	各クラウド リージョンは、クラウドの設定時に CCM UI で特定されます。CloudCenter プラットフォームで管理する必要があるクラウド リージョンごとに、GUAC、AMQP、および CCO コンポーネントをインストール、セットアップおよび設定する必要があります。

☐ 2.1	**AMQP**	• 非 HA
		  • CCM のホスト名（CCM Hostname）
		  • CCO のホスト名（CCO Hostname）
		• HA
		  • ***プライマリ AMQP***
		  • CCM のホスト名（CCM Hostname）
		  • CCO のホスト名（CCO Hostname）
		  • ***セカンダリ AMQP***
		  • CCM のホスト名（CCM Hostname）
		  • CCO のホスト名（CCO Hostname）

☐ 2.2	**CCO**	• 非 HA
		  • AgentBundle
		  • カスタム バンドルを使用する場合、cdn.cliqr.com をカスタム バンドル ストアの IP または DNS に置き換えます
		  • パッケージ ストアを使用する場合、repo.cliqrtech.com をカスタム パッケージ ストアの IP または DNS に置き換えます
		  • AMQP_Server
		  • AMQP Server IP
		  • AMQPポート（AMQP Port）
		  • ネットワーク：
		  • ホストネーム（Hostname）
		  • Guacamole
		  • Connection Broker Host
		  • Connection Broker Port1
		  • Connection Broker Port2
		  • Docker
		  • Docker Registry URL
		  • Docker CACert URL
		• CCO HA
		  • プライマリ CCO
		  • AgentBundle
		  • カスタム バンドルを使用する場合、cdn.cliqr.com をカスタム バンドル ストアの IP または DNS に置き換えます
		  • パッケージ ストアを使用する場合、repo.cliqrtech.com をカスタム パッケージ ストアの IP または DNS に置き換えます
		  • AMQP_Server
		  • AMQP Server IP
		  • AMQPポート（AMQP Port）
		  • ネットワークのホスト名
		  • Guacamole
		  • Connection Broker Host
		  • Connection Broker Port1
		  • Connection Broker Port2
		  • Docker
		  • Docker Registry URL
		  • Docker CACert URL
		  • CCO HA Info
		  • Primary CCO Node IP
		  • セカンダリ CCO ノード IP
		  • Tertiary CCO Node IP

☐ 3	モニタ（必須）	• 非 HA
		  • Monitor ID
		  • CCM Hostname/URL
		  • Monitor User

☐ 4	リポジトリ（条件付き）	• **パッケージ ストア**：リポジトリの IP アドレス/FQDN • **バンドル ストア**：インターネットへの接続が制限されている環境の場合は、ローカル バンドル ストアを作成して CCO に登録します。

フェーズ 1：インフラストラクチャの準備

- ハードウェア要件
- クラウドの微妙な違い
- 仮想アプライアンスのプロセス
- 前提条件チェッカー JSON ファイル

ハードウェア要件

CloudCenter プラットフォームには、企業向けに管理する VM インスタンスの数に基づく特定のハードウェア要件があります。このセクションで指定されたルート ディスク サイズに基づいて各アプライアンスを起動できます。

CCM、CCO、モニタ、およびリポジトリのハードウェア要件

VM の合計数	単一コンポーネントのハードウェア要件
500 未満	2 CPU、4 GB メモリ、50 GB ストレージ

501 ～ 2000	2 CPU、8 GB メモリ、100 GB ストレージ
2001 ～ 10000	4 CPU、16 GB メモリ、200 GB ストレージ
10000 超	4 CPU、32 GB メモリ、500 GB ストレージ

この領域が必要な理由
必要なコンポーネントは、次の理由で指定された領域を必要とします。

- 各 CCM サーバは、PostgreSQL データベース用の領域が必要です。
- 各 CCO サーバは、MongoDB データベース用の領域が必要です。
- 各監視サーバは、CCM および CCO サーバのために生成されるログ ファイル用の領域が必要です。
- 各リポジトリ サーバは条件付きであり、専用サーバの企業要件に依存します。

AMQP ハードウェア要件

VM の合計数	単一コンポーネントのハードウェア要件
500 未満	2 CPU、4 GB メモリ、50 GB ストレージ
501 ～ 2000	2 CPU、8 GB メモリ、50 GB ストレージ
2001 ～ 10000	4 CPU、16 GB メモリ、50 GB ストレージ
10000 超	4 CPU、32 GB メモリ、50 GB ストレージ

ワーカー ハードウェア要件

企業の要件に依存し、選択するインスタンス タイプと使用するアプリケーションに基づきます。

インフラストラクチャをインストールする際のクラウド固有の微妙な違い

- Alibaba の微妙な違い
- AWS の微妙な違い
- Azure の微妙な違い
- Cisco UCSD の微妙な違い
- Dimension Data の微妙な違い
- Google の微妙な違い
- OpenStack の微妙な違い
- SoftLayer の微妙な違い
- VMware の微妙な違い

Alibaba の微妙な違い

- 各 Alibaba リージョンに利用可能なインスタンス タイプ

  各リージョンでサポートされるインスタンスはリージョンによって異なります。Alibaba SDK と Alibaba Web インターフェイスでは、各ゾーンにリストされるインスタンスが異なります。CCM UI を使用して新しいインスタンスを追加できます。詳細については、「インスタンス タイプの管理」を参照してください。

- サポートされるストレージ タイプ

  CloudCenter プラットフォームは Alibaba クラウドの 2 つのストレージ タイプをサポートします。

  - SSD クラウド ディスク
  - Ultra クラウド ディスク

- Alibaba クラウド環境への SSH 接続

  Alibaba クラウド環境への SSH キー アクセスは許可されていないため、次のようにインスタンスのパスワードを指定する必要があります。

  - Linux の場合：ルート パスワードを指定します。
  - Windows の場合：管理パスワードを指定します。

  詳細については、「Deployment Environment Defaults」>「 *Alibaba - Cloud and Network Settings*」を参照してください。

AWS の微妙な違い

- CCO、CCO_PRIMARY、CCO_SECONDARY、および CCO_TERTIARY では、プロビジョニングに IAM ロールベースのアカウントを使用する場合、IAM ロールを使用して CCO VM を起動します。

- マスター/スレーブ セットアップ用の仮想 IP(VIP)または Elastic IP(EIP)を有効にするために特定の IAM ロールを使用して、**MGMTPOSTGRES_MASTER** と **MGMTPOSTGRES_SLAVE** の VM を起動します。
  - 仮想 IP または Elastic IP の選択

    データベース HA のために IAM ロールの VIP または EIP を使用するガイドライン:

    - **VIP を使用**:
      - 同じ VPC から MGMTPOSTGRES_MASTER と MGMTPOSTGRES_SLAVE の両方を起動する場合。
      - VIP を使用している場合、VPC 内でのサブネットの 1 つから未使用の IP を選択します。
    - **EIP を使用**:
      - 別の VPC から MGMTPOSTGRES_MASTER と MGMTPOSTGRES_SLAVE の両方を起動する場合。
      - EIP を使用している場合、VPC としてスコープを使用して AWS クラウド コンソールから新しい IP を割り当てます。
      - 詳細については、「VPC peering」を参照してください。

  - VIP または EIP ポリシーに特有の IAM ロールの作成

ポリシー	IAM ロール
VIP	`{ "Version": "2012-10-17", "Statement": [{ "Action": [ "ec2:AssignPrivateIpAddresses", "ec2:UnassignPrivateIpAddresses", "ec2:DescribeInstances", "ec2:DescribeNetworkInterfaces" ], "Effect": "Allow", "Resource": "*" }] }`
EIP	`{ "Version": "2012-10-17", "Statement": [ { "Action": [ "ec2:DescribeInstances", "ec2:DescribeNetworkInterfaces", "ec2:AssociateAddress", "ec2:DisassociateAddress", "ec2:DescribeAddresses" ], "Effect": "Allow", "Resource": "*" } ] }`

- RDS サービスとしての PostgreSQL

  SA または HA モードで RDS サービスとして PostgreSQL をセットアップするには、「*Configuring HA for PostgreSQL Database on AWS*」を参照してください。

Azure の微妙な違い

- Azure RM
  1. Azure RM モードで CentOS VM を起動します。
  2. 「*フェーズ 2:ファイアウォール ルールの設定*」にリストされている、CCO の設定に必要なエンドポイントを追加します。
  3. コア インストーラ パッケージを使用して、「*クラウド リージョンごと(必須)*」>「*CCO(必須)*」にリストされているように CCO をセットアップします。
  4. 詳細については、「クラウドの設定」>「*Azure Resource Manager クラウドの設定*」を参照してください。

- Azure Classic
  1. Azure Classic モードで CentOS VM を起動します。
  2. 「*フェーズ 2: ファイアウォール ルールの設定*」にリストされている、CCO の設定に必要なエンドポイントを追加します。
  3. コア インストーラ パッケージを使用して、「*クラウド リージョンごと(必須)*」>「*CCO(必須)*」にリストされているように CCO をセットアップします。
  4. CCO をメタデータ サーバに登録します。

```
curl-XPOST-d"info={\"userData\":\"Azure,<CCM_IP>\",\"image\":\"ccm\",\"ma
chineType\":\"large\",\"osName\":\"Linux\",\"tenant\":\"admin\"}"-k
 https://mds.cliqrtech.com/0.1/meta-data/Azure/<CCO_HOST_NAME>
```

  5. 次のコマンドを発行して登録を確認します。上記のステップからデータが返される必要があります。

```
curl http://mds.cliqrtech.com/0.1/meta-data/Azure/<CCO_HOST_NAME>
```

  6. 詳細については、「クラウドの設定」>「*Azure Classic クラウドの設定*」を参照してください。

- Azure Pack
  1. Azure Pack モードで CentOS VM を起動します。
  2. 「*フェーズ 2: ファイアウォール ルールの設定*」にリストされている、CCO の設定に必要なエンドポイントを追加します。
  3. コア インストーラ パッケージを使用して、「*クラウド リージョンごと(必須)*」>「*CCO(必須)*」にリストされているように CCO をセットアップします。
  4. CCO をメタデータ サーバに登録します。

```
curl-XPOST-d"info={\"userData\":\"AzurePack,<CCM_IP>\",\"image\":\"ccm\",
\"machineType\":\"large\",\"osName\":\"Linux\",\"tenant\":\"admin\"}"-k
 https://mds.cliqrtech.com/0.1/meta-data/AzurePack/<CCO_HOST_NAME>
```

  5. 次のコマンドを発行して登録を確認します。上記のステップからデータが返される必要があります。

```
curl http://mds.cliqrtech.com/0.1/meta-data/AzurePack/<CCO_HOST_NAME>
```

  6. 詳細については、「クラウドの設定」>「*Azure Pack クラウドの設定*」を参照してください。

Cisco UCSD の微妙な違い

- Cisco UCSD リリースの互換性

  CloudCenter 4.6 は、次の UCSD リリースをサポートしています。

  - Cisco UCS Director リリース 5.1
  - Cisco UCS Director リリース 5.2
  - Cisco UCS Director リリース 5.3

- 設定要件
  - 企業内で UCSD を統合する場合は、エンドツーエンドの導入を実行するための UCSD 環境に対するアクセス権が CloudCenter プラットフォームに必要です。
  - 1 つの CloudCenter で 1 つの UCSD インスタンスをサポートします。
  - CloudCenter の UCSD の各実装には、関連付けられた物理イメージのエントリが CloudCenter プラットフォーム内に必要です(このエントリは、論理イメージが使用されない場合でも、ダミーのプレースホルダとなります)。
  - 詳細については、「クラウドの設定」>「*Cisco UCSD クラウドの設定*」を参照してください。

Dimension Data の微妙な違い

- 設定要件

  次の要件に対応することを確認します。

  - VM を起動できる有効な Dimension Data CloudControl アカウント。
  - Dimension Data アカウントへのログインに使用される Dimension Data のアカウント名とパスワード。

Google の微妙な違い

- CCO インスタンスを起動した後

  keys フォルダ内の GCE .p12 ファイルをダウンロードして保存するには、次の手順に従います。

  1. /usr/local/osmosix/ フォルダに移動します。
  2. **/gce** というフォルダを作成します。
  3. **/usr/local/osmosix/gce** フォルダ内に、**keys** というフォルダを作成します。
  4. .p12 ファイルを **/usr/local/osmosix/gce/keys** フォルダにダウンロードします。

OpenStack の微妙な違い

マスター/スレーブ セットアップ用の仮想 IP（VIP）を使用して、**MGMTPOSTGRES_MASTER** と **MGMTPOSTGRES_SLAVE** の VM を起動します（「*インストールの概要*」を参照）。

- OpenStack サーバにアクセスできる VM にインストールされた OpenStack Neutron クライアントへのアクセス
  1. OpenStack のコマンドライン クライアントをインストールします。
  2. **MGMTPOSTGRES_MASTER** と **MGMTPOSTGRES_SLAVE VM** を起動します

- ポートの更新
  1. VIP マスター/スレーブ セットアップ用の未使用の IP を特定します。
  2. 次のコマンドを使用して、この IP で新しいポートを作成します。

     ```
     `neutron port-create --fixed-ip ip_address=<VIP> <network-name>`
     ```

  3. MGMTPOSTGRES_MASTER と MGMTPOSTGRES_SLAVE VM のポートの ID を取得します。

     ```
     `neutron port-list`
     ```

  4. **fixed_ips** の MGMTPOSTGRES_MASTER および MGMTPOSTGRES_SLAVE IP に対応するリストから **id** をメモします。
  5. 前のステップでメモした各ポート ID に対して次のコマンドを実行し、VIP を使用して MGMTPOSTGRES_MASTER と MGMTPOSTGRES_SLAVE に関連付けられているポートを更新します。

     ```
     `neutron port-update <port-id> --allowed-address-pairs
     type=dict list=true ip_address=<VIP>`
     ```

- ホスト名の設定

  起動されたすべての VM で、ホスト名を目的のホスト名に更新します。ロールに一致するホスト名を選択します。たとえば、*CCM_SA_PRIMARY.mydomain.com* です。

  PCS 認証が失敗する原因になるので、データベース サーバのホスト名にアンダースコアを含めることはできません。

  VM のインストールおよび設定後にホスト名を変更すると、未知の問題を引き起こす可能性があります。

- ホスト名の解決の設定

  ホスト名を更新したら、次のコマンドを実行して、VM ホスト名が解決可能であることを確認してください。

  ```
  hostname -i
  ```

  VM の名前が解決可能であれば、**/etc/hosts** ファイルを編集し、VM のホスト名を追加します。例を示します。*<hostname> 127.0.0.1*

- ネットワーク ルーティングのループバック

  ネットワーク ルーティングのループバックは CCM を参照します。これは指定した導入の NAT の背後にあり、内部ネットワークのサーバは外部 IP を使用して CCM にアクセスできないという制限があります。

  このシナリオでは、登録した CCO と AMQP サーバの /etc/hosts ファイルに行を追加して、CCM の内部プライベート IP を提供する必要があります。

次に例を示します。

CCM DNS 名が *ccm.example.com* で、NAT の背後にあり、内部プライベート IP アドレスが 12.16.0.5 で、外部パブリック IP アドレスが 54.1.2.5 である場合、ローカルの /etc/hosts ファイルに次の行を入力します

12.16.0.5 ccm.example.com

> 上記の例で使用したホスト名（ccm.example.com）はフェーズ 4 で CCM を設定する際に、***Public DNS*** として設定されているものと一致させる必要があります。

SoftLayer の微妙な違い

- CCO インスタンスを起動する前に

  SoftLayer デバイスと同じクラウド リージョンで CCO を起動する必要があります。CCO とこのデバイスに異なるリージョンを選択することはできません。

  詳細については、「クラウドの設定」>「*SoftLayer クラウドの設定*」を参照してください。

VMware の微妙な違い

vCenter

vCenter ユーザに完全な管理者権限がない場合は、（CloudCenter を使用する）各ユーザに少なくとも次のアクセス許可があることを確認してください。

vCenter オブジェクト	必要なアクセス許可	理由（Reason）
ネットワーク（Network）	ネットワークの割り当て	テンプレート/スナップショットのデフォルトのネットワークを変更する必要がある場合
データストア	領域の割り当て	永続的なディスク操作のため
	データストアの参照	
	低レベルのファイル操作	
	ファイルの削除	
フォルダ	フォルダの作成	ユーザのフォルダの作成のため
リソース	推奨事項の適用	データストア クラスタのサポートのため
	リソース プールへの VM の割り当て	リソース プールの選択のため
タスク	タスクの作成	VM の操作のため
	タスクの更新	
仮想マシン	すべてのアクセス許可	

詳細については、「クラウドの設定」>「*VMware クラウドの設定*」を参照してください。

仮想アプライアンスのセットアップ プロセス

サポートされる仮想アプライアンス

CloudCenter のメジャー リリースには、次のコンポーネントおよびクラウド プロバイダー用のアプライアンスが含まれています。これらのアプライアンスは、シスコにより、CentOS 7.x ベース イメージ上に構築されています。詳細については、「Virtual Appliances」を参照してください。

クラウド	イメージタイプ
Amazon	共有イメージ（AMI）
Azure RM	VHD
OpenStack	QCOW2
VMware	OVA
Google	共有イメージ
SoftLayer	共有イメージ

一般的な仮想アプライアンス アプローチ

アプライアンス アプローチのためにインフラストラクチャを準備するには、次の手順に従います。

1. CloudCenter コンポーネントごとのハードウェア要件を確認し、各コンポーネントの要件を満たしていることを確認します。
2. インストール シナリオを確認するために使用する必要がある JSON 記述子を準備します（このセクションで後述する「*CloudCenter 記述子 JSON ファイル*」を参照）。
3. ファイアウォール ルールの設定を行います。
4. イメージをダウンロードします。ダウンロードできるイメージと共有する必要があるイメージを確認するには、「Virtual Appliances」を参照してください。次に例を示します。

クラウド固有のアプライアンス	詳細（Details）
Amazon	cloudcenter-ami-request メーラー リストに電子メールを送信して、AWS アカウントの起動権限を取得します。
OpenStack	各コンポーネント用の QCOW2 イメージ ファイルをインポートします。
VMware	*CliqrTemplates* という名前のフォルダを作成し、各コンポーネント用の OVA ファイルをインポートします。
Google	cloudcenter-ami-request メーラー リストに電子メールを送信して、Google アカウントの起動権限を取得します。
SoftLayer（Bluemix）	cloudcenter-ami-request メーラー リストに電子メールを送信して、Bluemix アカウントの起動権限を取得します。
Azure RM	各コンポーネントの VHD ファイルをダウンロードします。

5. インポート済み/共有アプライアンス イメージを使用して、各コンポーネントのインスタンスを作成します。
   a. 1 つの CCM、モニタ、およびリポジトリ（専用サーバの条件付き）は、各 CloudCenter セットアップに必要です。

   > ワーカー イメージは CCM で定義されるため、このコンポーネントのインスタンスを起動する必要はありません。

   b. クラウド リージョンごとに 1 つの AMQP と CCO が必要です。
6. 起動したすべての仮想マシンのホスト名を設定し、ホスト名を更新します。この手順は、CloudCenter コンポーネントごとの IP アドレスの代わりに DNS 名を使用する場合に必要です。IP アドレスを使用する場合はこの手順をスキップできます。
   a. ロールに一致するホスト名を選択します。次に例を示します。

   例

   ```
   CCM.mydomain.com
   ```

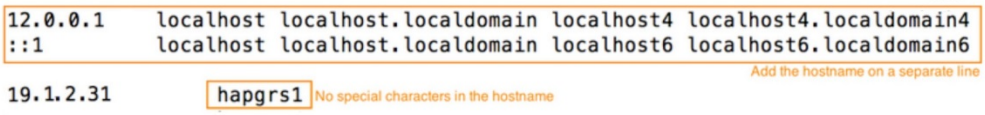
   > **VM のインストールおよび設定後にホスト名を変更すると、未知の問題を引き起こす可能性があります。**

   b. ホスト名を設定したら、次のコマンドを実行して、VM ホスト名が解決可能であることを確認してください。
      i. **hostname**
      ii. VM の名前が解決可能であれば、**/etc/hosts** ファイルを編集し、VM のホスト名を追加します。
      次に例を示します。

      例

      ```
      <hostname> 12.10.12.1
      ```

      iii. **/etc/hosts** ファイルで*ホスト名が解決可能*であることを確認します。
      - **/etc/hosts** ファイルにホスト名とコンポーネントの IP アドレスを追加します。



- 認証が失敗する原因となるため、データベース サーバでホスト名にアンダースコア、ハイフン、スペースを含む特殊文字を含めることはできません。
- ホスト名をローカルホストと同じ行にすることはできません。**/etc/hosts** ファイル内の別の行にホスト名を追加します。

7. ネットワーク ルーティングのループバック:
   - ネットワーク アドレス変換(NAT)の背後で実行中の導入済みの CCM を参照します。
   - この設定では、内部ネットワークからのマシンが CCM へのアクセスに外部 IP を使用しないように制限されます。
   - この制限に対処するため、CCO および AMQP サーバの **/etc/hosts** ファイルに行を追加し、CCM の内部プライベート IP を含める必要があります。例:CCM の DNS 名が ccm.example.com で、NAT の背後にあり、内部プライベート IP アドレスが 192.168.20.5 で、その外部パブリック IP アドレスが 54.16.20.5 の場合、ローカルの /etc/hosts ファイルに次の行を入力します。

例

```
192.168.20.5 ccm.example.com
```

CCM を設定する場合、上記で使用されるホスト名(ccm.example.com)は、CCM の設定時に ***Public DNS*** として設定したものと一致する必要があります。

クラウド固有のセットアップの詳細

- VMware アプライアンスのセットアップ

VMware アプライアンスのセットアップ

VMware クラウド用の CloudCenter アプライアンスを使用してインフラストラクチャを準備するには、次のプロセスに従います。

1. VMware コンソールで *CliqrTemplates* という名前のフォルダを作成し、各コンポーネント用の OVA ファイルをインポートします。
2. 各コンポーネントのイメージを起動する準備を行います。
3. インポートしたイメージを使用して各コンポーネントのインスタンスを起動します。
4. 各イメージのインスタンスを起動したら、以下を行います。
   a. イメージの電源をオンにします。
   b. ルート ユーザとしてイメージにログインします。

```
Username: root
Password: welcome2cliqr
sudo -i
```

続行する前に
この認証は汎用のクレデンシャルを使用します。最初のログイン後は、管理者アカウントの電子メールアドレスとパスワードを必ず変更してください。

5. ホスト名の設定:起動したすべての VM で、ホスト名を更新します。「仮想アプライアンスの概要」の*ロール*と一致するホスト名を選択します。*次に例を示します。*
   a. ホスト名:起動したすべての VM で、ホスト名を更新します。

コンポーネントをインストールして設定した*後*は、不明な問題が発生する場合があるため、ホスト名を変更しないでください。

ロールに一致するホスト名を選択します。次に例を示します。

例

```
CCM.mydomain.com
```

b. ホスト名の解決の設定：ホスト名を更新したら、次のコマンドを実行して、VM ホスト名が解決可能であることを確認します。
   i. **hostname -i**
   ii. VM の名前が解決可能であれば、**/etc/hosts** ファイルを編集し、VM のホスト名を追加します。次に例を示します。

例

```
<hostname> 127.0.0.1
```

c. ネットワーク ルーティングのループバック：
   i. ネットワーク アドレス変換（NAT）の背後で実行中の導入済みの CCM を参照します。
   ii. この設定では、内部ネットワークからのマシンが CCM へのアクセスに外部 IP を使用しないように制限されます。
   iii. この制限に対処するため、CCO および AMQP サーバの **/etc/hosts** ファイルに行を追加し、CCM の内部プライベート IP を含める必要があります。例：CCM の DNS 名が ccm.example.com で、NAT の背後にあり、内部プライベート IP アドレスが 192.168.20.5 で、その外部パブリック IP アドレスが 54.16.20.5 の場合、ローカルの /etc/hosts ファイルに次の行を入力します。

例

```
192.168.20.5 ccm.example.com
```

CCM を設定する場合、上記で使用されるホスト名（ccm.example.com）は、***Public DNS*** として設定したものと一致する必要があります。

d. CloudCenter 記述子 JSON ファイルの作成：すべての CloudCenter コンポーネントのインフラストラクチャを設定したら、CloudCenter 記述子 JSON ファイルを作成し、そこには、すべての CloudCenter コンポーネントを、各モードおよびロールのインフラストラクチャ要素に対応したモードおよび IP アドレスとともに表示します。この記述子ファイルは、ネットワーク コンプライアンス チェック（ステップ 3）で使用されます。次に、いくつかの一般的なコンポーネント モードの組み合わせに基づくサンプル ファイル記述子を示します。

全体的なファイル構造は、さまざまなコンポーネントのモード、クラウド リージョンの数、条件付き/オプションのコンポーネントの使用、およびリポジトリなどの要因によって異なります。また、ファイルで使用されているリージョン名は一意にする必要がありますが、クラウドやデータセンターの名前と一致する必要はありません。これらの文字列は、次に示すように、ネットワーク コンプライアンス チェックの実行、およびレポート結果にのみ使用されます。

JSON ファイルの例

```
{
    "CloudCenterComponents":
        { "CCM": {
            "CCM_IP": "CCM.Company1.com",
            "mode": "NON-HA "
        },
        "CloudRegions":
            [{ "components"
            : {
                "AMQP": {
                    "AMQP_IP": "AMQP.Company1.com",
                    "mode": "NON-HA"
                },
                "CCO": {
                    "CCO_IP": "CCO.Company1.com",
                    "mode": "NON-HA"
                }
            },
            "name": "AWSEast"
        }],
        "REPOS": {
            "BUNDLE_STORE": "http://cdn.cliqr.com",
            "DOCKER_REGISTRY": "http://repo.cliqrtech.com:5000",
            "PACKAGE_STORE": "http://repo.cliqrtech.com"
        }
    }
}
```

- OpenStack アプライアンスのセットアップ

OpenStack アプライアンスのセットアップ

OpenStack クラウド用の CloudCenter アプライアンスを使用してインフラストラクチャを準備するには、次のプロセスに従います。

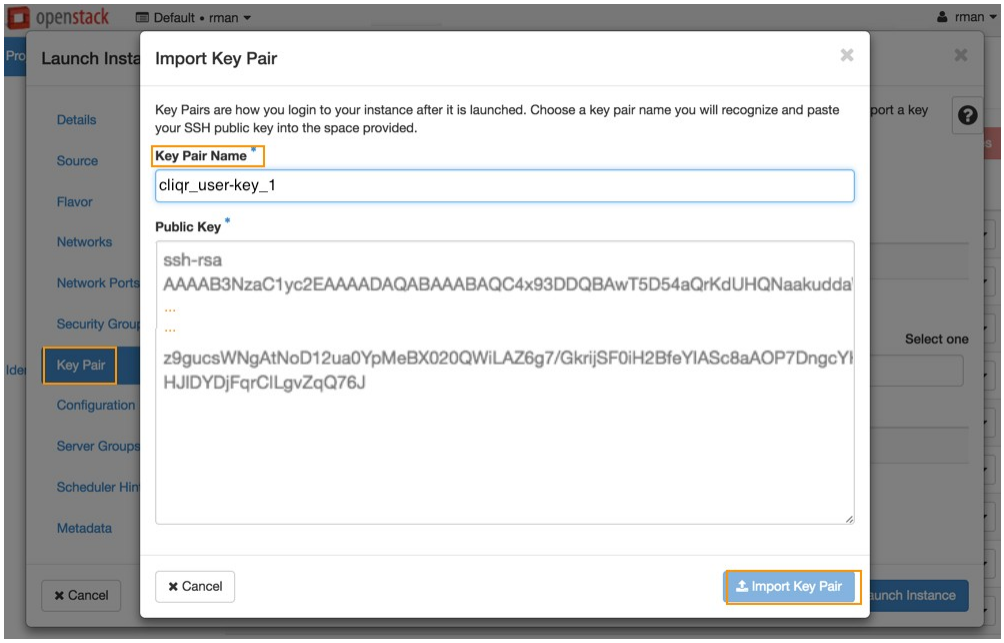
1. CloudCenter QCOW2 イメージを OpenStack コンソールにインポートします。
2. インポートしたイメージを使用して各コンポーネントのインスタンスを起動します。
3. 各 VM と関連付けし、さまざまなコンポーネント間の通信を有効にするようにセキュリティ グループを設定します。

> このページのネットワーク設定は、コンポーネントの相互通信のためのポートの最小要件について示しています。すべてのコンポーネントがすべてのポートを介して相互に通信できる環境（通常は POC 環境またはプライベート データセンター）ではこのフェーズを省略できます。
>
> 実稼働環境は、このセクションで指定されたポート経由でのみ通信できるようにすることで、セキュリティで保護されます。

「フェーズ 2：ファイアウォール ルールの設定」の表では、各コンポーネント ロールのネットワーキング要件を示しています。

4. 新規または既存のキー ペアを選択して各インスタンスにログインします。複数のキー ペアが利用可能な場合は、CloudCenter インスタンスに使用するものを *1 つ選択*する必要があります。

> キー ペアを選択しない場合、コンポーネント VM にログインできません。



- OpenStack コンソールから既存のキー ペアを選択します。
- 新しいキー ペアをインポートします。次の認証の詳細を使用して、キー ペア情報にアクセスします。
  - ユーザ名：**centos**
  - キー：OpenStack コンソールでインスタンスの起動に使用するキー。次のコマンドを使用して、サーバからキー ペアを取得し、OpenStack クラウド コンソールに貼り付けます。

```
$ cat my-public-key.pub
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQC4x93DDQBAwT5D54aQrKdUHQNaakudd
aWZxpcYfQCTL
...
...
/fHJlDYDjFqrCILgvZqQ76J
```

プライベート ネットワークをインスタンスに追加したら、キー ペアを正しく挿入したことを確認してください。

5. ホスト名の設定：起動したすべての VM で、ホスト名を更新します。「仮想アプライアンスの概要」の*ロール*と一致するホスト名を選択します。次に例を示します。
   a. ホスト名：起動したすべての VM で、ホスト名を更新します。

コンポーネントをインストールして設定した*後*は、不明な問題が発生する場合があるため、ホスト名を変更しないでください。

ロールに一致するホスト名を選択します。次に例を示します。

例

```
CCM.mydomain.com
```

   b. ホスト名の解決の設定：ホスト名を更新したら、次のコマンドを実行して、VM ホスト名が解決可能であることを確認します。
      i. **hostname**
      ii. VM の名前が解決可能であれば、**/etc/hosts** ファイルを編集し、VM のホスト名を追加します。
      次に例を示します。

例

```
12.168.20.5 ccm.example.com
```

iii. また、OpenStack の場合、ホスト名がサーバの再起動で変更されないことを確認する必要があります。IP アドレスの代わりに DNS 名を必要とする各サーバ上の /etc/sysconfig/network ファイルにホスト名のエントリを追加します。

OpenStack の導入に必須

```
HOSTNAME=<hostname>
```

c. ネットワーク ルーティングのループバック:
   i. ネットワーク アドレス変換(NAT)の背後で実行中の導入済みの CCM を参照します。
   ii. この設定では、内部ネットワークからのマシンが CCM へのアクセスに外部 IP を使用しないように制限されます。
   iii. この制限に対処するため、CCO および AMQP サーバの **/etc/hosts** ファイルに行を追加し、CCM の内部プライベート IP を含める必要があります。例:CCM の DNS 名が ccm.example.com で、NAT の背後にあり、内部プライベート IP アドレスが 192.168.20.5 で、その外部パブリック IP アドレスが 54.16.20.5 の場合、ローカルの /etc/hosts ファイルに次の行を入力します。

例

```
192.168.20.5 ccm.example.com
```

CCM を設定する場合、上記で使用されるホスト名(ccm.example.com)は、CCM の設定時に ***Public DNS*** として設定したものと一致する必要があります。

d. CloudCenter 記述子 JSON ファイルの作成:
すべての CloudCenter コンポーネントのインフラストラクチャを設定したら、CloudCenter 記述子 JSON ファイルを作成し、そこには、すべての CloudCenter コンポーネントを、各モードおよびロールのインフラストラクチャ要素に対応したモードおよび IP アドレスとともに表示します。この記述子ファイルは、ネットワーク コンプライアンス チェック(ステップ 3)で使用されます。次に、いくつかの一般的なコンポーネント モードの組み合わせに基づくサンプル ファイル記述子を示します。

全体的なファイル構造は、さまざまなコンポーネントのモード、クラウド リージョンの数、条件付き/オプションのコンポーネントの使用、およびリポジトリなどの要因によって異なります。また、ファイルで使用されているリージョン名は一意にする必要がありますが、クラウドやデータセンターの名前と一致する必要はありません。これらの文字列は、次に示すように、ネットワーク コンプライアンス チェックの実行、およびレポート結果にのみ使用されます。

JSON ファイルの例

```
{
    "CloudCenterComponents":
        { "CCM": {
            "CCM_IP": "CCM.Company1.com",
            "mode": "NON-HA "
        },
        "CloudRegions":
            [{ "components"
            : {
                "AMQP": {
                    "AMQP_IP": "AMQP.Company1.com",
                    "mode": "NON-HA"
                },
                "CCO": {
                    "CCO_IP": "CCO.Company1.com",
                    "mode": "NON-HA"
                }
            },
            "name": "AWSEast"
        }],
        "REPOS": {
            "BUNDLE_STORE": "http://cdn.cliqr.com",
            "DOCKER_REGISTRY": "http://repo.cliqrtech.com:5000",
            "PACKAGE_STORE": "http://repo.cliqrtech.com"
        }
    }
}
```

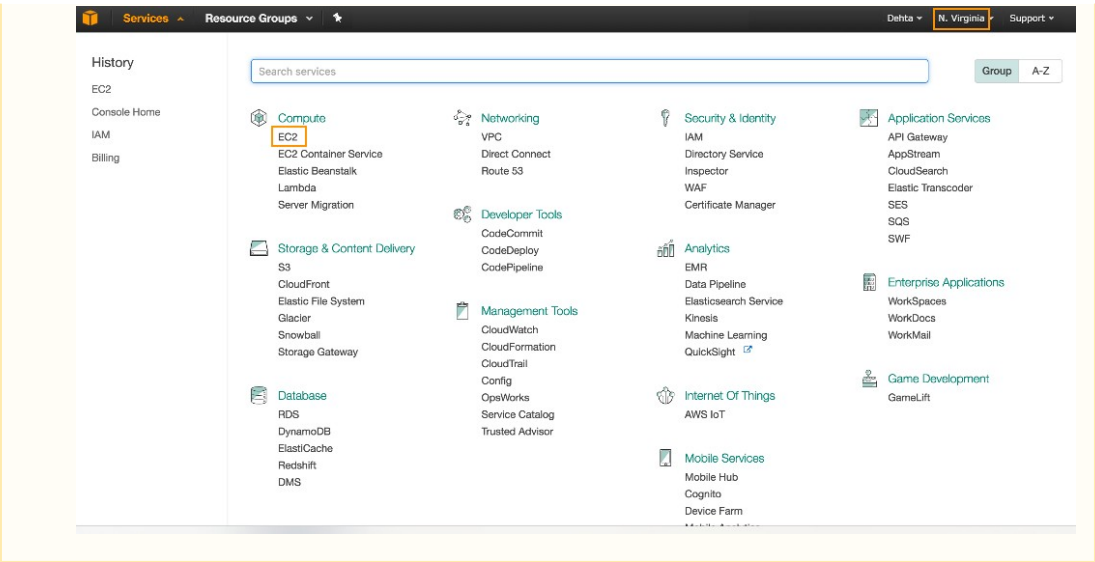
- Amazon アプライアンスのセットアップ

AWS アプライアンスのセットアップ

AWS クラウド用の CloudCenter アプライアンスを使用してインフラストラクチャを準備するには、次のプロセスに従います。

1. CloudCenter サポート ケース（https://mycase.cloudapps.cisco.com/case または http://www.cisco.com/c/en/us/support/index.html）を開くことによって AWS アカウントのイメージ共有を要求します。要求では以下の詳細を指定します。
    a. AWS アカウント番号
    b. CloudCenter のバージョン
    c. カスタマー ID（CID）
    d. 顧客名
    e. 実稼働または POC のセットアップ
    f. [連絡先電子メール（Contact email）]
2. ケースをオープンすると、共有 AMI ID でサポート ケースが更新されます。**AMI ID でサポート ケースが更新された後にのみ、次の手順に進みます。**
3. AWS クラウド コンソールに移動し、以下を選択します。
    a. リージョン：**US East (North Virginia)**
    b. コンピューティング：**EC2**

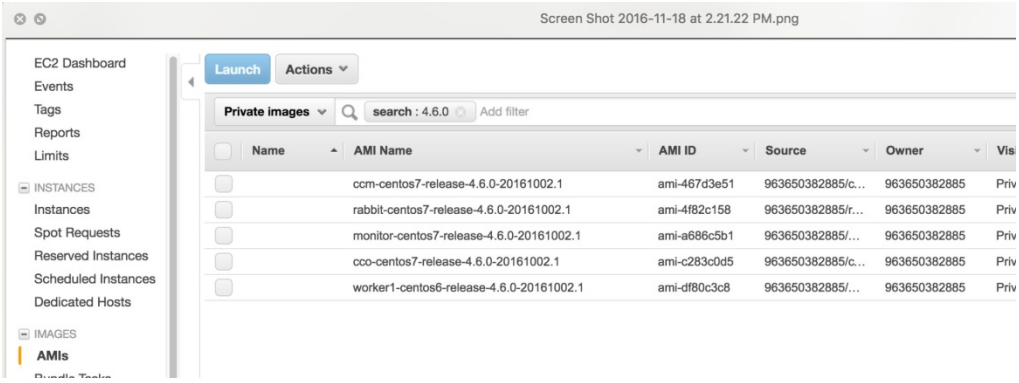
> **シスコ提供の AWS イメージ**
> デフォルトでは、シスコは US East（North Virginia）リージョンに対して*のみ*イメージを提供します。



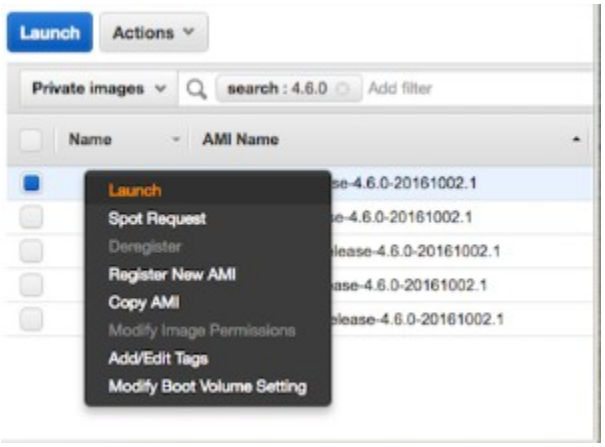
他のリージョンを使用する場合は、次の手順に従います。

i. 残りのプロセスに従って、シスコが提供する AMI を使用して各 CloudCenter コンポーネントを起動するように CloudCenter アプライアンスを設定します。
ii. 各コンポーネントを新しい AMI として保存します（詳細は AWS のドキュメントを参照）。
iii. 必要な AWS リージョンに AMI をコピーします（詳細は AWS のドキュメントを参照）。
iv. この残りのプロセスに従って、新しい AWS リージョンで CloudCenter アプライアンスを設定します。

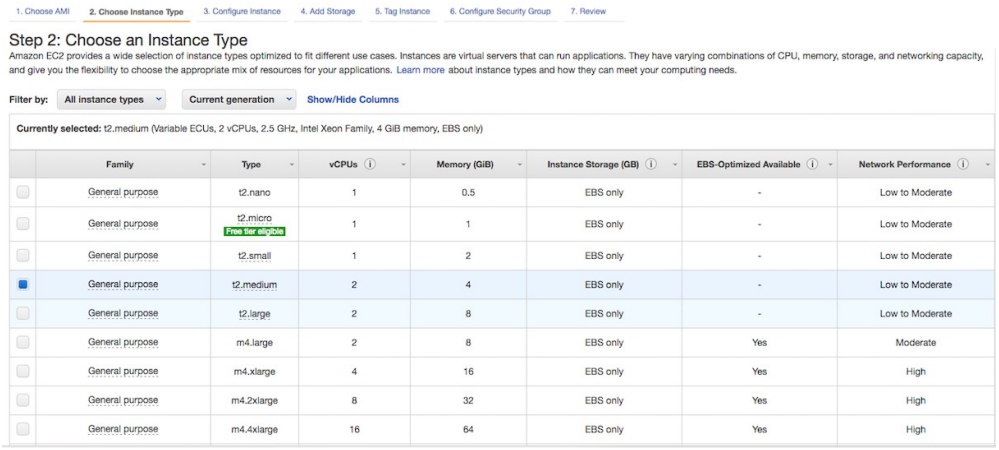
4. 各コンポーネントの AMI ID を特定します。
   a. 検索バーで [Private Images] を検索します。



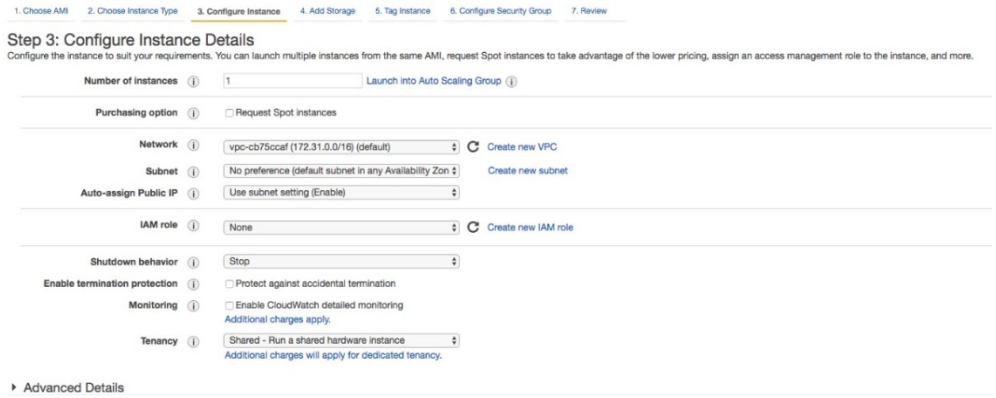
   b. 選択したプライベート イメージが、電子メールで送信された AMI ID に記載されているものと同じであることを確認します。
5. AMI ID を使用して各コンポーネントのインスタンスを起動します。



   a. インスタンス タイプを選択します（詳細については、「フェーズ 1：インフラストラクチャの準備」>「*ハードウェア要件*」を参照してください）。

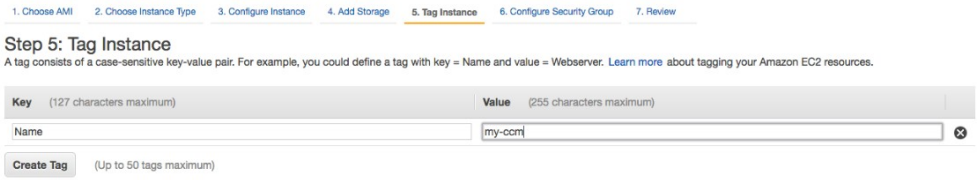


b. 環境の必要に応じてインスタンスの詳細を設定します。



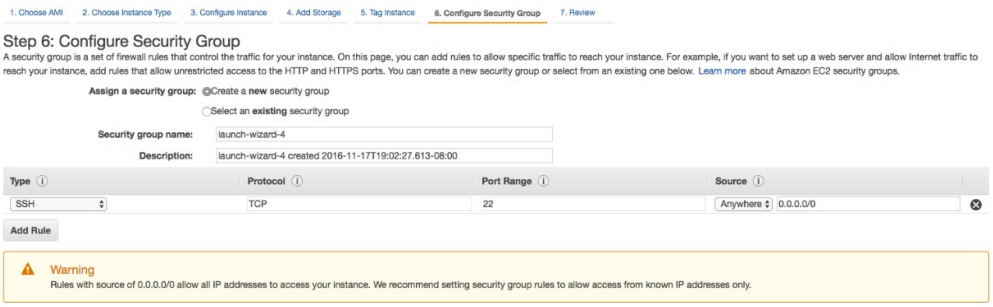
c. 任意のストレージを追加します。

d. 記述名を使用してインスタンスにタグ付けします。CloudCenter の名前については、「仮想アプライアンスの概要」のモードとロールを参照してください。

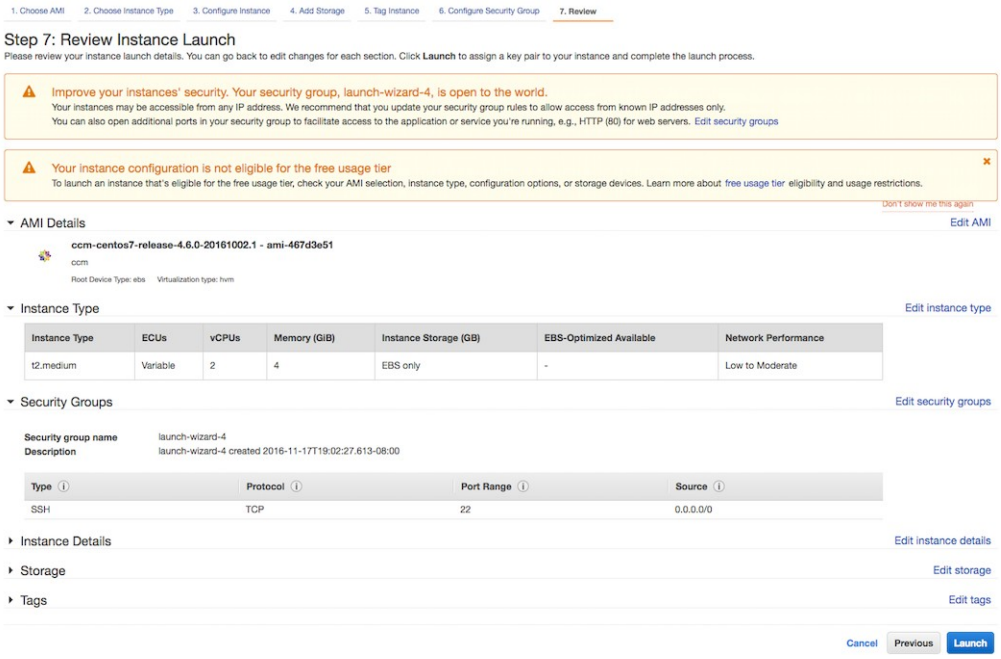


e. 各 VM と関連付けるセキュリティ グループを設定します。詳細については、「フェーズ 2:ファイアウォール ルールの設定」を参照してください。このプロセスの次のセクション「*ネットワーク ルールの設定*」では、最低限必要なネットワーク設定を示しています。

> コンポーネント VM への SSH アクセスを許可するようにポート 22 がオープンであることを確認します。

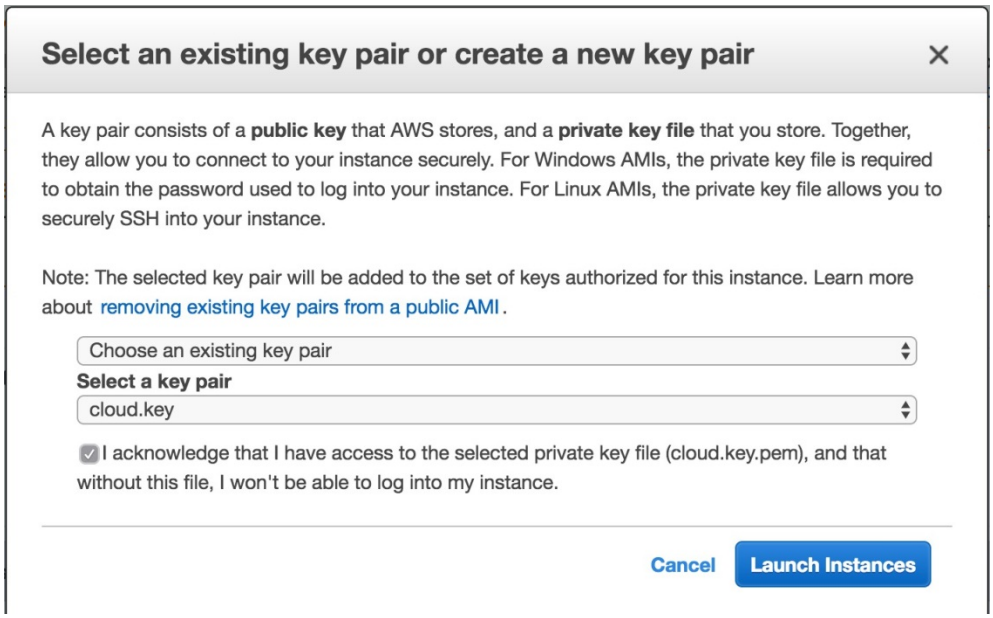


f. 環境の必要に応じてインスタンスの起動設定を確認して更新します。



g. [Launch] をクリックすると、[Select an existing key pair or create a new key pair] 画面が表示されます。キー ペアの詳細は、AWS のドキュメントを参照してください。

> キー ペアを選択しない場合、コンポーネント VM にログインできません。



h. [Launch Instance] をクリックしてコンポーネント VM を起動します。VM 起動プロセスの完了の AWS コンソールが正常に完了したことを確認します。

6. ホスト名の設定：起動したすべての VM で、ホスト名を更新します。「仮想アプライアンスの概要」の*ロール*と一致するホスト名を選択します。次に例を示します。
   a. ホスト名：起動したすべての VM で、ホスト名を更新します。

> コンポーネントをインストールして設定した*後*は、不明な問題が発生する場合があるため、ホスト名を変更しないでください。

> ロールに一致するホスト名を選択します。次に例を示します。

例

```
CCM.mydomain.com
```

b. ホスト名の解決の設定：ホスト名を更新したら、次のコマンドを実行して、VM ホスト名が解決可能であることを確認します。
   i. **hostname**
   ii. VM の名前が解決可能であれば、**/etc/hosts** ファイルを編集し、VM のホスト名を追加します。
   次に例を示します。

例

```
19.168.20.5 ccm.example.com
```

   iii. また、AWS の場合、サーバのリブート後もホスト名が変わらないように、**/etc/cloud/cloud.cfg** ファイルに次のエントリが含まれていることを確認する必要があります。

AWS の導入に必須

```
preserve_hostname: true
```

c. ネットワーク ルーティングのループバック：
   i. ネットワーク アドレス変換（NAT）の背後で実行中の導入済みの CCM を参照します。
   ii. この設定では、内部ネットワークからのマシンが CCM へのアクセスに外部 IP を使用しないように制限されます。
   iii. この制限に対処するため、CCO および AMQP サーバの **/etc/hosts** ファイルに行を追加し、CCM の内部プライベート IP を含める必要があります。例：CCM の DNS 名が ccm.example.com で、NAT の背後にあり、内部プライベート IP アドレスが 192.168.20.5 で、その外部パブリック IP アドレスが 54.16.20.5 の場合、ローカルの /etc/hosts ファイルに次の行を入力します。

例

```
192.168.20.5 ccm.example.com
```

CCM を設定する場合、上記で使用されるホスト名（ccm.example.com）は、CCM の設定時に ***Public DNS*** として設定したものと一致する必要があります。

7. CloudCenter 記述子 JSON ファイルの作成：すべての CloudCenter コンポーネントのインフラストラクチャを設定したら、CloudCenter 記述子 JSON ファイルを作成し、そこには、すべての CloudCenter コンポーネントを、各モードおよびロールのインフラストラクチャ要素に対応したモードおよび IP アドレスとともに表示します。この記述子ファイルは、ネットワーク コンプライアンス チェック（ステップ 3）で使用されます。次に、いくつかの一般的なコンポーネント モードの組み合わせに基づくサンプル ファイル記述子を示します。

全体的なファイル構造は、さまざまなコンポーネントのモード、クラウド リージョンの数、条件付き/オプションのコンポーネントの使用、およびリポジトリなどの要因によって異なります。また、ファイルで使用されているリージョン名は一意にする必要がありますが、クラウドやデータセンターの名前と一致する必要はありません。これらの文字列は、次に示すように、ネットワーク コンプライアンス チェックの実行、およびレポート結果にのみ使用されます。

JSON ファイルの例

```
{
    "CloudCenterComponents":
        { "CCM": {
            "CCM_IP": "CCM.Company1.com",
            "mode": "NON-HA "
        },
        "CloudRegions":
            [{ "components"
            : {
                "AMQP": {
                    "AMQP_IP": "AMQP.Company1.com",
                    "mode": "NON-HA"
                },
                "CCO": {
                    "CCO_IP": "CCO.Company1.com",
                    "mode": "NON-HA"
                }
            },
            "name": "AWSEast"
        }],
        "REPOS": {
            "BUNDLE_STORE": "http://cdn.cliqr.com",
            "DOCKER_REGISTRY": "http://repo.cliqrtech.com:5000",
            "PACKAGE_STORE": "http://repo.cliqrtech.com"
        }
    }
}
```

前提条件チェッカー JSON ファイル

仮想アプライアンスの概要のすべてについてインフラストラクチャを設定した後は、CloudCenter のすべてのコンポーネントを、各モードとロールのインフラストラクチャ要素に対応するコンポーネントのモードおよび IP アドレスとともにリストする CloudCenter 記述子 JSON ファイルを作成します。この記述子ファイルは、「フェーズ 3: 前提条件チェッカーの実行」で使用します。このセクションでは、コンポーネント モードの共通の組み合わせに基づき、サンプルの記述子ファイルを提供します。

JSON ファイルをローカルに保存します。

全体のファイル構造は次の要因によって異なります。

- 各コンポーネントのモード
- クラウド リージョンの数
- 条件/オプション コンポーネント、リポジトリなどの使用。
- このファイルで使用される固有のリージョン名。これらの名前は、すべてのクラウドやデータセンター名と一致する必要がないことに注意してください。これらの文字列は、ネットワーク コンプライアンス チェックの実行および結果のレポートにのみ使用されます

ローカル リポジトリ サーバを設定した場合は、バンドル ストア、パッケージ ストア、および Docker レジストリの値をサーバの値に置き換えます（セットアップに固有のその他の変更とともに）。設定していない場合は、次のサンプル記述子ファイルで使用されているデフォルト値を使用することができます。

DNS 名を設定した場合は、IP アドレスではなく、DNS 名を使用します。

- 記述子ファイル: 例 1

```
{
    "CloudCenterComponents":
        { "CCM": {
            "CCM_IP": "CCM.Company1.com",
            "mode": "NON-HA "
        },
        "CloudRegions":
            [{ "components"
            : {
                "AMQP": {
                    "AMQP_IP": "AMQP.Company1.com",
                    "mode": "NON-HA"
                },
                "CCO": {
                    "CCO_IP": "CCO.Company1.com",
                    "mode": "NON-HA"
                }
            },
            "name": "AWSEast"
        }],
        "REPOS": {
            "BUNDLE_STORE": "http://cdn.cliqr.com",
            "DOCKER_REGISTRY": "http://repo.cliqrtech.com:5000",
            "PACKAGE_STORE": "http://repo.cliqrtech.com"
        }
    }
}
```

- 記述子ファイル：例 2

```
{
    "CloudCenterComponents":
        { "CCM": {
            "CCM_SA_IP": "CCM.Company2.com",
            "MGMTPOSTGRES_IP": "MGMTPOSTGRES_SA.Company2.com",
            "mode": "STANDALONE"
        },
        "CloudRegions":
            [{ "components"
            : {
                "AMQP": {
                    "AMQP_IP": "AMQP.Company2.com",
                    "mode": "NON-HA"
                },
                "CCO": {
                    "CCO_IP": "CCO.Company2.com",
                    "mode": "NON-HA"
                }
            },
            "name": "AWSEast"
        }],
        "REPOS": {
            "BUNDLE_STORE": "http://cdn.cliqr.com",
            "DOCKER_REGISTRY": "http://repo.cliqrtech.com:5000",
            "PACKAGE_STORE": "http://repo.cliqrtech.com"
        }
    }
}
```

- 記述子ファイル：例 3

```
{
    "CloudCenterComponents": {
        "CCM": {
            "CCM_LB_IP": "169.0.1.1",
            "CCM_SA_PRIMARY_IP": "169.0.1.2",
            "CCM_SA_SECONDARY_IP": "169.0.1.3",
            "MGMTPOSTGRES_MASTER_IP": "169.0.1.4",
            "MGMTPOSTGRES_SLAVE_IP": "169.0.1.5",
            "MGMTPOSTGRES_VIP": "169.0.1.6",
            "mode": "HA"
        },
        "CloudRegions":
            [{ "components": {
                "AMQP": {
                    "AMQP_LB_IP": "169.0.1.7",
                    "AMQP_PRIMARY_IP": "169.0.1.8",
                    "AMQP_SECONDARY_IP": "169.0.1.9",
                    "mode": "HA"
                }, "CCO": {
                    "CCO_LB_IP": "169.0.1.10",
                    "CCO_PRIMARY_IP": "169.0.1.11",
                    "CCO_SECONDARY_IP": "169.0.1.12",
                    "mode": "HA"
                },
                "Dedicated_External_Script_Executor":
                    { "EXT_SCRIPT_EXECUTOR_IP": "169.0.1.13",
```

```
                "mode": "NON-HA"
            },
            "Dedicated_Guacamole_Server": {
                "GUAC_IP": "169.0.1.14",
                "mode": "NON-HA"
            }
        },
        "name": "AWSEast"
    }, {
        "components": {
            "AMQP": {
                 "AMQP_LB_IP": "169.0.1.15",
                "AMQP_PRIMARY_IP": "169.0.1.16",
                "AMQP_SECONDARY_IP": "169.0.1.17",
                 "mode": "HA"
            },
            "CCO": {
                 "CCO_LB_IP": "169.0.1.18",
                "CCO_PRIMARY_IP": "169.0.1.19",
                "CCO_SECONDARY_IP": "2.2.2.2",
                 "mode": "HA"
            },
            "Dedicated_External_Script_Executor": {
                "EXT_SCRIPT_EXECUTOR_IP": "169.0.1.20",
            "mode": "NON-HA"
            },
            "Dedicated_Guacamole_Server": {
                "GUAC_IP": "169.0.1.21",
                "mode": "NON-HA"
            }
        },
        "name": "MyOpenStack"
    }],
    "MON": {
        "MON": "169.0.1.22",
        "mode": "NON-HA"
    },
    "REPOS": {
        "BUNDLE_STORE": "http://cdn.cliqr.com",
        "DOCKER_REGISTRY": "http://repo.cliqrtech.com:5000",
        "PACKAGE_STORE": "http://repo.cliqrtech.com"
```

```
            }
        }
    }
```

フェーズ 2: ファイアウォール ルールの設定

- ファイアウォール ルールの概要
- CCM ファイアウォール ルール
- CCO ファイアウォール ルール
- AMQP ファイアウォール ルール
- モニタ ファイアウォール ルール
- リポジトリ ファイアウォール ルール

ファイアウォール ルール

- 概要
- 前提条件
- セキュリティ グループ
- プロキシの設定
- Firewalld

概要

このフェーズでは、さまざまなコンポーネント間の通信を可能にするファイアウォール/ネットワーク ルールを設定する必要があります。

> このページのネットワーク設定は、コンポーネントの相互通信のためのポートの最小要件について示しています。
>
> 実稼働環境は、このセクションで指定されたポート経由でのみ通信できるようにすることで、セキュリティで保護されます。

> すべてのコンポーネントがすべてのポートを介して相互に通信できる環境（通常は POC 環境またはプライベート データセンター）では、企業要件に基づいてファイアウォール ルールまたはセキュリティ グループを設定する必要があります。外部ネットワークや公開されているインターネットに対して不必要なポートを公開しないでください。

> CloudCenter コンポーネントごとに、入力と出力の両方のルールを設定する場合があります。
>
> 出力ルールですべてのトラフィックをオープンにし（IP アドレスの範囲を 0.0.0.0/0 に設定）、すべてのブラウザが各 VM にアクセスできるようにする場合は、各コンポーネントの出力ルール ポート要件に従う必要はありません。

前提条件

次のタスクが完了済みである必要があります。

1. 各ネットワーク アーキテクチャの例で使用されるポートについて、「仮想アプライアンスの概要」>「*モード*」で提供されている情報を読みます。
2. 環境で HA を設定する場合は、「高可用性のベスト プラクティス」を理解します。

   > 各コンポーネントのロード バランサ（LB）は、CloudCenter の観点からはサードパーティ アプリケーションです。各 CloudCenter コンポーネントのロード バランサを設定するときは、「*高可用性のベスト プラクティス*」で示された LB の要件に準拠することを確認してください。

3. 各クラウドについて、「フェーズ 1: インフラストラクチャの準備」で示されたクラウド固有の微妙な違いに従います。
4. すでに各コンポーネントのポートを設定している場合は、次の情報に基づいて**各コンポーネントのポート設定を修正**する必要がありことがあります。
   a. このページで後述する「*セキュリティ グループ*」、「*プロキシ設定*」、および「*Firewalld*」のセクションで指定された情報。
   b. 各 CloudCenter コンポーネント（LB を含む）のファイアウォール ルール要件：
      - *CCM ファイアウォール ルール*
      - *CCO ファイアウォール ルール*
      - *AMQP ファイアウォール ルール*
      - *モニタ ファイアウォール ルール*

セキュリティ グループ

AWS または OpenStack の場合、ネットワーク ルールはセキュリティ グループを使用して設定されます。

- すべてのポートの要件は TCP プロトコルを使用します。唯一の例外は、UDP プロトコルを使用するポート 5405 です（「*CCM ファイアウォール ルール*」を参照）。
- コンポーネントと HTTPS アクセスの間のすべての通信では、SSL プロトコルとして TLS を使用します。

一度正確にセキュリティ グループを設定すると、JSON ファイルはエラーなく渡されます。

プロキシの設定

インターネットへの接続にプロキシ サーバが必要な場合は、「*フェーズ 4:コンポーネントのインストール*」の CCM と CCO サーバのプロキシ設定を設定していることを確認してください。

FirewallD

CloudCenter コンポーネントのロード バランサを設定する場合は、firewalld がデフォルトで有効になっていることに注意してください。CloudCenter コンポーネントがロード バランサと通信できるようにするには、明示的に無効にする必要があります。

CCM ファイアウォール ルール

- CCM ポート
- CCM_SA ポート
- CCM_SA_PRIMARY および CCM_SA_SECONDARY ポート
- MGMTPOSTGRES ポート
- MGMTPOSTGRES_MASTER と MGMTPOSTGRES_SLAVE ポート
- CCM_LB ポート

CCM ポート

ポート	方向（Direction）	リモート送信元	注記（Notes）
22	入力（オプション）	許可された SSH の送信元 IP	トラブルシューティングの目的。
80	入力（オプション）	0.0.0.0/0（またはアクセス可能なユーザ ブラウザでの適切な IP アドレス範囲）	HTTP から HTTPS へのリダイレクション用。
443	受信側	0.0.0.0/0（またはアクセス可能なユーザ ブラウザでの適切な IP アドレス範囲）	UI/API アクセス用。
4560	送信側	Monitor	ELK 通信用 - Elasticsearch ポート。
5671	入力/出力（オプション）	ESB API 通信	CCM の ESB AMQP モジュールとの双方向通信用。このポートは、AMQP モジュールへのプログラムによるアクセスを確立する必要がある場合にオープンにする必要があります。ESB の機能を使用する場合にのみ必要です。
8443	受信側	• CCO または • CCO_PRIMARY、CCO_SECONDARY、および CCO_TERTIARY • Monitor • AMQP または • AMQP_PRIMARY と AMQP_SECONDARY	次の間の双方向通信用: • CCO と CCM • モニタと CCM CloudCenter の導入でサポートされるすべてのクラウド リージョンに必要です。
	送信側	• CCO または • CCO_LB • Monitor	AMQP から CCM への一方向通信用。
8881	送信側	Monitor	ELK 通信用 - Logstash ポート。
15672	入力/出力（オプション）	ESB UI 通信	CCM の ESB AMQP モジュールとの双方向通信用。このポートは、AMQP UI から AMQP モジュールへのアクセスを確立する必要がある場合にオープンにする必要があります。ESB の機能を使用する場合にのみ必要です。

CCM_SA ポート

ポート	方向（Direction）	リモート送信元	注記（Notes）
22	入力（オプション）	許可された SSH の送信元 IP	トラブルシューティングの目的。
80	入力（オプション）	0.0.0.0/0（またはアクセス可能なユーザ ブラウザでの適切な IP アドレス範囲）	HTTP から HTTPS へのリダイレクション用。
443	受信側	0.0.0.0/0（またはアクセス可能なユーザ ブラウザでの適切な IP アドレス範囲）	UI/API アクセス用。
4560	送信側	Monitor	ELK 通信用 - Elasticsearch ポート。
5432	送信側	MGMTPOSTGRES	データベースへの通信用。
5671	入力/出力（オプション）	ESB API 通信	CCM の ESB AMQP モジュールとの双方向通信用。このポートは、AMQP モジュールへのプログラムによるアクセスを確立する必要がある場合にオープンにする必要があります。ESB の機能を使用する場合にのみ必要です。
8443	受信側	• CCO または • CCO_PRIMARY、CCO_SECONDARY、および CCO_TERTIARY • Monitor • AMQP または • AMQP_PRIMARY と AMQP_SECONDARY	次の間の双方向通信用: • CCO と CCM • モニタと CCM CloudCenter の導入でサポートされるすべてのクラウド リージョンに必要です。
	送信側	• CCO または • CCO_LB • Monitor	AMQP から CCM への一方向通信用。
8881	送信側	Monitor	ELK 通信用 - Logstash ポート。
15672	入力/出力（オプション）	ESB UI 通信	CCM の ESB AMQP モジュールとの双方向通信用。このポートは、AMQP UI から AMQP モジュールへのアクセスを確立する必要がある場合にオープンにする必要があります。ESB の機能を使用する場合にのみ必要です。

CCM_SA_PRIMARY および CCM_SA_SECONDARY ポート

ポート	方向（Direction）	リモート送信元	注記（Notes）
22	入力（オプション）	許可された SSH の送信元 IP	トラブルシューティングの目的。
	入力/出力	• CCM • CCM_SA_PRIMARY または • CCM_SA_SECONDARY	CCO/AMQP 設定ウィザードから CCM をリモートで設定するため。
			CCM プライマリおよびセカンダリ VM 間の静的ファイル同期用。
80	入力（オプション）	0.0.0.0/0（またはアクセス可能なユーザ ブラウザでの適切な IP アドレス範囲）	HTTP から HTTPS へのリダイレクション用。
443	受信側	CCM_LB	UI/API アクセス用。
4560	送信側	Monitor	ELK 通信用 - Elasticsearch ポート。
5432	送信側	MGMTPOSTGRES	データベースへの通信用。
5671	入力/出力（オプション）	ESB API 通信	CCM の ESB AMQP モジュールとの双方向通信用。このポートは、AMQP モジュールへのプログラムによるアクセスを確立する必要がある場合にオープンにする必要があります。ESB の機能を使用する場合にのみ必要です。
5703	入力/出力	• CCM_SA_PRIMARY または • CCM_SA_SECONDARY	HA のデータの処理の内部実装用。

8443	受信側	• CCO または • CCO_PRIMARY、CCO_SECONDARY、および CCO_TERTIARY • CCM_LB • Monitor • AMQP または • AMQP_PRIMARY と AMQP_SECONDARY	次の間の双方向通信用: • CCO と CCM • モニタと CCM CloudCenter の導入でサポートされるすべてのクラウド リージョンに必要です。 AMQP から CCM への一方向通信用。
	送信側	• CCO または • CCO_LB • Monitor	
8881	送信側	Monitor	ELK 通信用 - Logstash ポート。
15672	入力/出力(オプション)	ESB UI 通信	CCM の ESB AMQP モジュールとの双方向通信用。このポートは、AMQP UI から AMQP モジュールへのアクセスを確立する必要がある場合にオープンにする必要があります。ESB の機能を使用する場合にのみ必要です。

MGMTPOSTGRES ポート

ポート	方向(Direction)	リモート送信元	注記(Notes)
22	入力(オプション)	許可された SSH の送信元 IP	トラブルシューティングの目的。
5432	受信側	CCM_SA	CCM スタンドアロン VM からの着信接続用。

MGMTPOSTGRES_MASTER と MGMTPOSTGRES_SLAVE ポート

ポート	方向(Direction)	リモート送信元	注記(Notes)
22	入力(オプション)	許可された SSH の送信元 IP	トラブルシューティングの目的。
	入力/出力	MGMTPOSTGRES_MASTER と MGMTPOSTGRES_SLAVE	MGMTPOSTGRES マスター/スレーブ VM 間の静的ファイル同期用。
2224 3121	入力/出力	MGMTPOSTGRES_MASTER と MGMTPOSTGRES_SLAVE	高可用性を実現するための両方のデータベース VM 間の Pacemaker クラスタリング用。
5432	受信側	CCM_SA_PRIMARY と CCM_SA_SECONDARY	CCM スタンドアロン VM からの着信接続用。
	入力/出力	MGMTPOSTGRES_MASTER と MGMTPOSTGRES_SLAVE	マスターとスレーブのデータベース VM 間の通信用。
5405 (UDP)	入力/出力	MGMTPOSTGRES_MASTER と MGMTPOSTGRES_SLAVE	高可用性を実現するための Corosync Cluster Engine グループの通信システム用。
21064	入力/出力	MGMTPOSTGRES_MASTER と MGMTPOSTGRES_SLAVE	高可用性を実現するための両方のデータベース VM 間の Pacemaker クラスタリング用。

CCM_LB ポート

ポート	方向(Direction)	リモート送信元	注記(Notes)
22	入力(オプション)	許可された SSH の送信元 IP	トラブルシューティングの目的。
80	入力(オプション)	0.0.0.0/0(またはアクセス可能なユーザ ブラウザでの適切な IP アドレス範囲)	HTTP から HTTPS へのリダイレクション用。
443	受信側	0.0.0.0/0(またはアクセス可能なユーザ ブラウザでの適切な IP アドレス範囲)	UI/API アクセス用。
	送信側	CCM_SA_PRIMARY と CCM_SA_SECONDARY	CCM プライマリおよびセカンダリ VM 間の通信用。
8443	送信側	CCM_SA_PRIMARY と CCM_SA_SECONDARY	CCM プライマリおよびセカンダリ VM 間の通信用。
	受信側	• CCO または • CCO_PRIMARY、CCO_SECONDARY、および CCO_TERTIARY • Monitor • AMQP または • AMQP_PRIMARY と AMQP_SECONDARY	CCO、AMQP、およびモニタ VM からの通信用。

CCO ファイアウォール ルール

- CCO ポート
- CCO_PRIMARY、SECONDARY、および TERTIARY ポート
- CCO_LB ポート

CCO ポート

ポート	方向（Direction）	リモート送信元	注記（Notes）
すべて（All）	出力（条件付き）	クラウド リージョンのエンドポイント、スクリプト ソース	クラウド リージョンのエンドポイント アクセスと外部サービスで定義されているスクリプト/パッケージのダウンロード用。
22	入力（オプション）	許可された SSH の送信元 IP	トラブルシューティングの目的。
4560	送信側	Monitor	ELK 通信用 - Elasticsearch ポート。
8443	入力/ 送信側	• CCM または • CCM_SA または • CCM_SA_PRIMARY と CCM_SA_SECONDARY	CCO と CCM VM 間の双方向通信用。
	受信側	• Monitor • AMQP または • AMQP_PRIMARY と AMQP_SECONDARY	CCO 通信用。
8881	送信側	Monitor	ELK 通信用 - Logstash ポート。

CCO_PRIMARY、SECONDARY、および TERTIARY ポート

ポート	方向（Direction）	リモート送信元	注記（Notes）
すべて（All）	出力（条件付き）	クラウド リージョンのエンドポイント、スクリプト ソース	クラウド リージョンのエンドポイント アクセスと外部サービスで定義されているスクリプト/パッケージのダウンロード用。
22	入力（オプション）	許可された SSH の送信元 IP	トラブルシューティングの目的。
	入力/出力	• CCO_PRIMARY • CCO_SECONDARY • CCO_TERTIARY	CCM/AMQP 設定ウィザードから CCO をリモートで設定するため。
4560	送信側	Monitor	ELK 通信用 - Elasticsearch ポート。
5701	入力/出力	CCO_PRIMARY CCO_SECONDARY CCO_TERTIARY	HA のデータの処理の内部実装用。
8443	受信側	• Monitor • AMQP または • AMQP_PRIMARY と AMQP_SECONDARY • CCO_LB	CCO 通信用。
8881	送信側	Monitor	ELK 通信用 - Logstash ポート。
27017	受信側	CCO_PRIMARY CCO_SECONDARY CCO_TERTIARY	MongoDB 接続用

CCO_LB ポート

ポート	方向（Direction）	リモート送信元	注記（Notes）
22	入力（オプション）	許可された SSH の送信元 IP	トラブルシューティングの目的。
8443	受信側	• CCM または • CCM_SA または • CCM_SA_PRIMARY と CCM_SA_SECONDARY • AMQP_PRIMARY と AMQP_SECONDARY • Monitor	CCM VM から CCO への通信用。
	送信側	CCO_PRIMARY、CCO_SECONDARY、および CCO_TERTIARY	CCO のロード バランサから CCO VM への通信用。

AMQP ファイアウォール ルール

- AMQP ポート
- AMQP_PRIMARY と AMQP_SECONDARY ポート
- AMQP_LB ポート

AMQP ポート

ポート	方向（Direction）	リモート送信元	注記（Notes）
22	入力（オプション）	許可された SSH の送信元 IP	トラブルシューティングの目的。
443	受信側	0.0.0.0/0（またはアクセス可能なユーザ ブラウザでの適切な IP アドレス範囲）	起動された VM の SSH/VNC および RDP アクセス用。
5671	受信側	• CCO または • CCO_PRIMARY、CCO_SECONDARY、および CCO_TERTIARY • ワーカー VM IP の範囲	CCO VM からの通信および起動された VM からの通信用。
7788	入力/出力	AMQP	起動された VM の SSH/VNC アクセス用。リバース プロキシによる実行。ループバック接続のリバース プロキシによる実行。
7789	受信側	ワーカー VM IP の範囲	起動された VM の SSH/VNC アクセス用。ループバック接続のリバース プロキシによる実行。
8443	送信側	• CCM または CCM_SA または CCM_LB • CCO または CCO_LB	起動された VM の SSH/VNC アクセス用。AMQP VM の Guacamole サーバはこのポートによって CCM および CCO VM と通信します。

AMQP_PRIMARY と AMQP_SECONDARY ポート

ポート	方向（Direction）	リモート送信元	注記（Notes）
22	入力（オプション）	許可された SSH の送信元 IP	トラブルシューティングの目的。
	入力/出力	AMQP_PRIMARY と AMQP_SECONDARY	AMQP インスタンスを別の AMQP インスタンスからリモートで設定するため。
443	受信側	AMQP_LB	起動された VM の SSH/VNC および RDP アクセス用。
4369	入力/出力	AMQP_PRIMARY と AMQP_SECONDARY	AMQP プライマリおよびセカンダリ VM 間の通信用。
5671	受信側	• CCO または CCO_LB • ワーカー VM IP の範囲 • AMQP_LB	CCO VM からの通信および起動された VM からの通信用
7788	入力/出力	AMQP_LB	起動された VM の SSH/VNC アクセス用。ループバック接続のリバース プロキシによる実行。
7789	受信側	ワーカー VM IP の範囲	起動された VM の SSH/VNC アクセス用。ループバック接続のリバース プロキシによる実行。
8443	送信側	• CCM または CCM_SA または CCM_LB • CCO または • CCO_LB	起動された VM の SSH/VNC アクセス用。AMQP の Guacamole サーバはこのポートで CCM および CCO と通信します。
25672	入力/出力	AMQP_PRIMARY と AMQP_SECONDARY	AMQP プライマリおよびセカンダリ VM 間の通信用。

AMQP_LB ポート

ポート	方向（Direction）	リモート送信元	注記（Notes）
22	入力（オプション）	許可された SSH の送信元 IP	トラブルシューティングの目的。
443	受信側	0.0.0.0/0（またはアクセス可能なユーザ ブラウザでの適切な IP アドレス範囲）	起動された VM の SSH/VNC アクセス用。リバース プロキシによる実行。
	送信側	AMQP_PRIMARY と AMQP_SECONDARY	

5671	受信側	• CCO または • CCO_PRIMARY、CCO_SECONDARY、および CCO_TERTIARY • アプリケーション（ワーカー）VM IP の範囲	CCO VM からの通信および起動された VM からの通信用。
	送信側	AMQP_PRIMARY と AMQP_SECONDARY	AMQP プライマリおよびセカンダリ VM 間の通信用。
7788	受信側	AMQP_PRIMARY と AMQP_SECONDARY	起動された VM の SSH/VNC アクセス用。ループバック接続のリバース プロキシによる実行。
7789	受信側	ワーカー VM IP の範囲	起動された VM の SSH/VNC アクセス用。ループバック接続のリバース プロキシによる実行。

モニタ ファイアウォール ルール

MON ポート

ポート	方向（Direction）	リモート送信元	注記（Notes）
22	入力（オプション）	許可された SSH の送信元 IP	トラブルシューティングの目的。
4560	受信側	• CCM または CCM_SA_PRIMARY と CCM_SA_SECONDARY • CCO または CCO_PRIMARY、CCO_SECONDARY、および CCO_TERTIARY	（Logstash）CCM や CCO にログを収集、処理、プッシュするため。
8881	受信側	• CCM または CCM_SA_PRIMARY と CCM_SA_SECONDARY • CCO または CCO_PRIMARY、CCO_SECONDARY、および CCO_TERTIARY	（Elasticsearch）CCM や CCO のログをダウンロードするため。
8882	受信側	パブリック ブラウザ アクセス	Kibana コンソールでログを表示するため。
8443	入力/出力	• CCM または • CCM_SA または • CCM_SA_PRIMARY、CCM_SA_SECONDARY、および CCM_LB	CCM およびモニタ VM 間の双方向通信用。
	送信側	CCO または CCO_LB	CCO VM へのアクセス用。

リポジトリ ファイアウォール ルール

リポジトリ ポート

ポート	方向（Direction）	リモート送信元	注記（Notes）
22	入力（オプション）	許可された SSH の送信元 IP	SSH アクセス用。
	送信側	パブリック リポジトリ サーバ: repo.cliqrtech.com	すべての OS、コンポーネントとサービス パッケージの同期用
80	受信側	すべてのコンポーネントとワーカー VM IP の範囲	アプリケーション VM（ワーカー）のブートストラップ スクリプトとエージェント パッケージのダウンロード用
[5000]	受信側	ワーカー VM IP の範囲	アプリケーション VM（ワーカー）のコンテナ サービスのイメージのダウンロード用

フェーズ 3: 前提条件チェッカーの実行

ネットワーク通信

すべてのファイアウォール ルールが、さまざまな CloudCenter コンポーネント、ワーカー、VM およびエンドユーザ アクセス全体で相互通信用に正しく設定されていることを確認するために、前提条件チェッカーを実行する必要があります。

CloudCenter のコンポーネント VM

CloudCenter のすべてのコンポーネントについて、ネットワーク コンプライアンス チェックを行うには、「*フェーズ 1: インフラストラクチャの準備*」の一部として起動されるすべての仮想マシンで次の手順を実行します。

1. 「*フェーズ 1: インフラストラクチャの準備*」で作成したデプロイメント記述子 JSON ファイルを /tmp の場所にアップロードします。
2. **network_validator.py**（CloudCenter インストーラ ファイルで利用可能）ファイルと呼ばれるバリデータ スクリプトを /tmp の場所にアップロードします。
3. 次のコマンドを /tmp の場所から実行します。

```
python
network_validator.py --role=<role> --region=<unique region
identifier> --deploymentDetails=<envdeployment descriptor JSON
file path>
```

次にこのコマンドの実行例を示します。

- ```
  python
  network_validator.py --role=CCM --deploymentDetails=deployment.json
  ```

- ```
  python
  network_validator.py --role=CCO_PRIMARY --region=AmazonEast1
  --deploymentDetails=deployment.json
  ```

- ```
  python
  network_validator.py --role=AMQP_LB --region=AmazonEast1
  --deploymentDetails=deployment.json
  ```

4. 各 CCM、CCO、AMQP コンポーネントの network_validator.py スクリプトを実行した後、cloudcenter_validator.json という名前のファイルが、CCM、CCO、AMQP サーバの /tmp の場所に作成されます。次の例は、CCM 用に作成された cloudcenter_validator.json ファイルです。

```
[{
    "TO_ROLE": "CCO",
    "region": "AWSEast",
    "TO_IP": "12.1.4.5",
    "PORT": 8443,
    "RESULT": "Success"
}, {
    "TO_ROLE": "PACKAGE_STORE",
    "TO_IP": "repo.cliqrtech.com",
    "PORT": 80,
    "RESULT": "Success"
}]
```

5. 次の点を確認するには、このコマンドの結果を確認してください。
   - 障害は発生しませんでした。障害が発生した場合、ネットワーク設定を適切に更新して、テストを繰り返します。
   - すべての必須ネットワーク ルールが正しく設定されました。

アプリケーション（ワーカー）VM

アプリケーション オーケストレーション プロセスの一部として起動されるアプリケーション VM が関連する CloudCenter のコンポーネントとリポジトリと通信できるようにするために、ネットワーク コンプライアンス チェックも実行する必要もあります。

すべてのアプリケーション VM にネットワーク コンプライアンス チェックを実行するには、次の手順を実行します。

1. CloudCenter プラットフォームにより管理されることを意図された任意のクラウド環境のテスト仮想マシンを起動します
```

2. 「*フェーズ 1: インフラストラクチャの準備*」で作成したデプロイメント記述子 JSON ファイルを /tmp の場所にアップロードします。
3. /tmp の場所に network_validator.py ファイルというバリデータ スクリプトをアップロードします。
4. 次のコマンドを /tmp の場所から実行します。

```
python network_validator.py --role=AGENT --region=<unique region identifier>
--deploymentDetails=<deployment descriptor JSON file path>
```

次にこのコマンドの実行例を示します。

```
python network_validator.py
--role=AGENT --region=AmazonEast1 --deploymentDetails=deployment.json
```

5. 次の点を確認するには、このコマンドの結果を確認してください。
   - 障害は発生しませんでした。障害が発生した場合、ネットワーク設定を適切に更新して、テストを繰り返します。
   - すべての必須ネットワーク ルールが正しく設定されました。
6. すべてのコンプライアンス チェックが成功したことを確認した後で、すべてのテスト VM を終了します。

クライアント テスト

一部の CloudCenter のコンポーネント（たとえば、CCM、AMQP、GUAC）は CloudCenter UI（*CCM UI* または *UI* ともいいます）にアクセスするエンドユーザがアクセス可能であるか、CloudCenter REST API を呼び出す必要があります。このようなコンポーネントへのクライアント アクセスを確認するには、次の手順を実行します。

1. エンドユーザが CloudCenter プラットフォームを管理する元のネットワークで実行している Linux、Windows（Python 対応）または MacOSX システムを特定します。
2. このクライアント マシンにデプロイメント記述子 JSON ファイルをアップロードします。
3. このクライアント マシンに network_validator.py ファイルをアップロードします。
4. Python スクリプトの場所から次のコマンドを実行します。

```
python network_validator.py --role=CLIENT  --deploymentDetails=deployment.json
```

5. 次の点を確認するには、このコマンドの結果を確認してください。
   - 障害は発生しませんでした。障害が発生した場合、ネットワーク設定を適切に更新して、テストを繰り返します。
   - すべての必須ネットワーク ルールが正しく設定されました。

重要:
「*フェーズ 4: CloudCenter のコンポーネントのインストールと設定*」に進む前に、ネットワーク コンプライアンス チェックがすべて正常であることを確認します。

無視することができる唯一のエラーは、Docker レジストリ接続に関するものです。

```
Component DOCKER_REGISTRY IP repo.cliqrtech.com:5000 Port 5000 is not open!
```

フェーズ 4: コンポーネントの設定

- フェーズ 4 の概要
- CCM（必須）
- モニタ（必須）
- リポジトリ（条件付き）
- クラウド リージョンごと（必須）
- ワーカー（条件付き）

設置および設定の概要

> **インストール方法**
> フェーズ 4 を開始する前に、この時までにフェーズ 1、2、および 3 を完了する必要があります。これらのフェーズを完了していない場合は、「インストール方法」に戻ってこのプロセスの現在地を確認してください。

インストール タスク

ここでは、各 CloudCenter コンポーネントで次のタスクを完了するようにするインストール プロセスについて説明します。

1. （各コンポーネントで特定される）必要なファイルを software.cisco.com からダウンロードします。詳細については、「仮想アプライアンスの概要」を参照してください。
2. 各コンポーネントの *アプライアンス*を実行します。

順序	コンポーネント	クラウド リージョンごとか、導入単位か	仮想アプライアンスは使用可能か	必須かどうか
1	CCM	導入単位	はい（CentOS 7）	必須（Required）
2	Monitor	導入単位	はい（CentOS 7）	必須（Required）
3	Repo	導入単位	はい（CentOS 7）	必須（インターネット アクセスがない場合）
4	CCO	クラウド リージョンごと	はい（CentOS 7）	必須（Required）
5	AMQP	クラウド リージョンごと	はい（CentOS 7）	必須（Required）
6	アプリケーション VM（ワーカー）のカスタム イメージ	クラウド リージョンごと	はい（CentOS 6）	動的ブートストラップをサポートしないクラウドでは必須（「Base OS Images」で示されるとおり）

3. ウィザードを起動し、コンポーネントのプロパティを設定します。

アプライアンスを使用する CCM のインストール（必須）

- CCM 非 HA

アプライアンスを使用する CCM 非 HA のインストール

- プロキシの設定
- CCM ウィザードのプロパティの設定

プロキシの設定

インターネットへの接続にプロキシ サーバが必要な場合は、CCM と CCO サーバのプロキシ設定で Tomcat Service を設定していることを確認してください。

プロキシ サーバを使用してインターネットに接続するには、次の手順を実行します。

1. プロキシ設定を反映するようにプロキシ環境を変更します。
2. /usr/local/tomcat/bin/setenv.sh ファイルでは、既存の **JAVA_OPTS** 環境変数に次のパラメータを追加することが CloudCenter プラットフォームにより要求されます。

HTTP の場合に必須 - JAVA_OPTS 環境変数に次のパラメータを追加します

```
-Dhttp.proxyHost=<proxy_hostname> -Dhttp.proxyPort=<port_number>
```

または

HTTPS の場合に必須 - JAVA_OPTS 環境変数に次のパラメータを追加します

```
-Dhttps.proxyHost=<proxy_hostname> -Dhttps.proxyPort=<port_number>
```

JAVA_OPTS にパラメータが追加された /usr/local/tomcat/bin/setenv.sh の例

```
export LD_LIBRARY_PATH=/usr/local/apr/lib
export CATALINA_PID=$CATALINA_HOME/catalina.pid
export JPDA_ADDRESS=8000
export JAVA_OPTS="-Djava.awt.headless=true -Dfile.encoding=UTF-8 -server
-Xms1024m -Xmx2048m -XX:NewSize=512m -XX:MaxNewSize=512m
-XX:PermSize=512m -Dhttp.proxyHost=proxy.cisco.com -Dhttp.proxyPort=80"
export CATALINA_OUT=/dev/null
```

3. CCM または CCO サーバがプロキシをバイパスしてネットワーク リソースに到達する必要がある場合、追加のパラメータが必要になることがあります。

```
-Dhttp.nonProxyHosts=<bypass_hostname>
```

オプション - プロキシをバイパスする /usr/local/tomcat/bin/setenv.sh の例

```
export LD_LIBRARY_PATH=/usr/local/apr/lib
export CATALINA_PID=$CATALINA_HOME/catalina.pid
export JPDA_ADDRESS=8000
export JAVA_OPTS="-Djava.awt.headless=true -Dfile.encoding=UTF-8 -server
-Xms1024m -Xmx2048m -XX:NewSize=512m -XX:MaxNewSize=512m
-XX:PermSize=512m -Dhttp.proxyHost=proxy.cisco.com -Dhttp.proxyPort=80
-Dhttp.nonProxyHosts=10.1.1.1"
export CATALINA_OUT=/dev/null
```

4. Tomcat サービスを再起動します。

```
/etc/init.d/tomcat stop
/etc/init.d/tomcat start
```

5. **ps aux | grep java** コマンドを発行することによって、プロキシ設定が有効であることを確認します。

ps aux | grep java コマンドの出力

```
cliqrus+ 25106 0.0 45.3 4368868 929000 ? Sl Mar02 54:15
/usr/lib/jvm/java-8-sun/bin/java
-Djava.util.logging.config.file=/usr/local/tomcatgua/conf/logging.propert
ies -Djava.util.logging.manager=org.apache.juli.ClassLoaderLogManager
-Djava.awt.headless=true -Dfile.encoding=UTF-8 -server -Xms1024m
-Xmx2048m -XX:NewSize=512m -XX:MaxNewSize=512m -XX:PermSize=512m
-XX:MaxPermSize=512m -Djav.endorsed.dirs=/usr/local/tomcatgua/endorsed
-classpath
/usr/local/tomcatgua/bin/bootstrap.jar:/usr/local/tomcatgua/bin/tomcat-ju
li.jar -Dcatalina.base=/usr/local/tomcatgua
-Dcatalina.home=/usr/local/tomcatgua
-Djava.io.tmpdir=/usr/local/tomcatgua/temp
-Dhttp.proxyHost=proxy.cisco.com -Dhttp.proxyPort=80
-Dhttp.nonProxyHosts=10.1.1.1 org.apache.catalina.startup.Bootstrap start
```

出力に、**-Dhttp.proxyHost=proxy.cisco.com -Dhttp.proxyPort=80 -Dhttp.nonProxyHosts=10.1.1.1** の行が存在することを確認します。

CCM ウィザードのプロパティの設定

CCM ウィザードのプロパティを設定するには、次の手順に従います。

1. CCM ウィザードを起動するには、次のプロセスに従います。
   a. CCM インスタンスに *CentOS* ユーザとして SSH 接続します。
   b. 次のコマンドを実行します。

```
sudo -i
```

2. CCM ウィザードを起動します。

CCM ウィザードのパス

```
/usr/local/cliqr/bin/ccm_config_wizard.sh
```

サーバのプロパティを設定します。

> **今後の参照のためにこれを書き留めてください。**
> 後で使用できるように、「*インストール方法*」>「*メモ*」セクションを印刷したものにフィールドの詳細を書き留めてください。

ウィザード メニュー	フィールド	説明
メール（Mail） メール通知を送信する SMTP サーバの詳細。デフォルト設定を保持する場合、SMTP サーバの詳細は設定しません。	SMTP ホスト（SMTP Host）	smtp.gmail.com
	SMTP ポート（SMTP Port）	デフォルトは 465 です
	SMTP 認証（SMTP Auth）	ブール値の設定 • True = SMTP サーバでは認証が必要です。 • False = SMTP サーバでは認証が必要ありません。

Mail_User メール通知を送信するメール認証と設定の詳細。デフォルト設定を保持する場合、メール機能は設定せず、電子メールは送信されません。	メール ユーザ（Mail User）	SMTP サーバの電子メールアドレス
	パスワード（Password）	SMTP サーバへのログイン パスワード
	ユーザから（From User）	CCM サーバから電子メールを送信する電子メールアドレス（返信なし）
	表示名（Display Name）	CCM サーバから電子メールを送信するときに表示される名前
Server_info（必須）	パブリック DNS（Public DNS）	CCM の DNS（または IP アドレス）：CCM VM との通信に CCO VM によって使用されます。
	モニタ URL（Monitor URL）	モニタ VM の完全な URL。例：https://<MON IP address>:8443 • HTTPS プロトコルが必要です。 • モニタ VM からのヘルス ステータスの取得に CCM VM で使用されます。
	Hazelcast IP	CCM VM のプライベート IP アドレス：CloudCenter プラットフォームによって内部で使用されます。HA モードでは必要です。
	外部 URL（External URL）	CCM サーバの CloudCenter 外部 URL。HA モードでは必要です。
Config_App_Logo アプリケーション プロファイル テンプレートで使用されます。	DB パスワード（DB Password）	CCM 非 HA アプライアンス モードでは、PostgreSQL データベースから自動的にこの情報を抽出します。 CCM HA アプライアンス モードではデータベースとしてこの情報を持たないため、相互に通信するためには CCM を両方設定する必要があります。そのため、データベース情報を提供することによってデータベースにアプリケーション プロファイル テンプレートの場所を明示的に設定する必要があります。 デフォルトの DB パスワード = *cliqr* ⚠ 初回ログイン後は、すぐにこのデフォルト パスワードを変更してください。詳細については、「PostgreSQL Password」を参照してください。
ESB_Info Enterprise Service Bus（ESB）、CloudCenter アプライアンスにデフォルトではインストールされないオプション コンポーネントをインストールした場合にのみ必要。	Rabbit ホスト	ESB AMQP サーバの IP アドレスまたはホスト名です。
	Rabbit ポート	5671
	[管理サーバ アドレス（Management Server Address）]	CCM サーバの IP アドレスまたはホスト名です。
	通知サーバ アドレス（Notification Server Address）	通知サーバの IP アドレスまたはホスト名です（CCM サーバと同じが理想）。
	信頼ストアのパスワード（Trust Store Password）	ESB インスタンスの信頼ストアのパスワードです。
	キー ストアのパスワード（Key Store Password）	ESB インスタンスのキー ストアのパスワード。
ネットワーク（Network）	ホストネーム（Hostname）	CCM サーバのホスト名：変更を行わない場合は、デフォルトを使用します。
DB	IP またはホスト名（IP or Hostname）	データベースの DNS または IP です。 • ローカル ホスト：デフォルト、flyway 移行設定は含まれません • リモート ホスト、flyway 移行設定が含まれます。この行の最後の項目を参照してください。
	[ユーザ名（Username）]	データベース（ローカルまたはリモート）の認証済みユーザ名。
	パスワード（Password）	データベース（ローカルまたはリモート）の認証済みパスワード。

	Flyway 移行（Flyway Migrate）	これはオプションです。リモート ホストは、リモート データベースの IP アドレスを提供することによって、リモート データベースに CCM を設定します。IP アドレスを提供すると、flyway 移行プロセスを設定するための追加の画面が表示されます。 • はい（Yes）：Flyway 移行が行われます。 • いいえ（No）：コンフィギュレーション ファイルのみが更新されます。 DB の設定は、スタンドアロン データベースの導入に必要です。
ELK_Info	ELK ホスト（ELK Host）	ELK ホスト（モニタ VM）の IP アドレスを指定します。
	Elasticsearch ポート（Elasticsearch Port）	8881 がデフォルトで表示されます。
	Logstash ポート（Logstash Port）	4560 がデフォルトで表示されます。
	Kibana ポート（Kibana Port）	8882 がデフォルトで表示されます。
	ELK ユーザ（ELK User）	デフォルトの ELK ユーザ名 = *logreader* です。
	ELK パスワード（Password）	デフォルトの ELK パスワードは *re@d0nly* です（d と n の間は *ゼロ*です）（このパスワードは初回ログイン後に変更してください。詳細については、「Download Log File」を参照してください）。
	ホスト識別子（Host Identifier）	サーバの一意の ID：固有識別子の前に必ず、**CCM_** を追加してください（CCM_1 など）
	ホスト識別子のリスト（Host Identifier List）	HA モードを使用する環境にのみ適用：HA セットアップのすべての ELK/モニタ ホストに対してカンマ区切りの一意のホスト識別子のリストを提供します（例：CCM_1,CCM_2,myCCM）。 HA モードで動作する環境では、それぞれの server.properties ファイルに CCM_1,CCM_2 として固有 ID が設定されている 2 つの CCM インスタンスがある場合、このプロパティは両方の CCM インスタンスで **CCM_1,CCM_2** と示す必要があります。各 CCM は HA モードの他の CCM の固有 ID を認識する必要があります。
Config_Certs：カスタム証明書メニュー	証明書の生成（Generate Certs）	• CloudCenter ID：この CloudCenter の導入を識別するために顧客に割り当てられた一意の英数字文字列。 • 会社名（Company Name）：この証明書が生成される会社の名前。
	証明書の更新（Update Certs）	証明書 Zip パス（Certs Zip Path）：certs.zip ファイルのパスを指定します。デフォルト パスは /tmp/certs.zip です。

3. CCM 設定ウィザードを終了します。
4. Tomcat Service を再起動して変更を適用するには、[はい（Yes）] を選択します。

CCM インスタンスは正常にインストールされました。*これで、次のステップに進むことができます。*

- ヘルス モニタ コンポーネントをインストールしている場合、「*ヘルス モニタ インストール*」を参照してください
- ヘルス モニタ コンポーネントをインストールしていない場合は、「*CloudCenter リージョンごとのインストール*」セクションにスキップし、クラウドごとの CloudCenter コンポーネントのインストールを続行します。

- CCM 非 HA スタンドアロン

アプライアンスを使用する非 HA スタンドアロン CCM のインストール

- プロキシの設定
- MGMTPOSTGRES：CCM_SA からの DB アクセスの設定
- CCM ウィザードのプロパティの設定

プロキシの設定

インターネットへの接続にプロキシ サーバが必要な場合は、CCM と CCO サーバのプロキシ設定で Tomcat Service を設定していることを確認してください。

プロキシ サーバを使用してインターネットに接続するには、次の手順を実行します。

1. プロキシ設定を反映するようにプロキシ環境を変更します。
2. /usr/local/tomcat/bin/setenv.sh ファイルでは、既存の **JAVA_OPTS** 環境変数に次のパラメータを追加することが CloudCenter プラットフォームにより要求されます。

HTTP の場合に必須 - JAVA_OPTS 環境変数に次のパラメータを追加します

```
-Dhttp.proxyHost=<proxy_hostname> -Dhttp.proxyPort=<port_number>
```

または

HTTPS の場合に必須 - JAVA_OPTS 環境変数に次のパラメータを追加します

```
-Dhttps.proxyHost=<proxy_hostname> -Dhttps.proxyPort=<port_number>
```

JAVA_OPTS にパラメータが追加された /usr/local/tomcat/bin/setenv.sh の例

```
export LD_LIBRARY_PATH=/usr/local/apr/lib
export CATALINA_PID=$CATALINA_HOME/catalina.pid
export JPDA_ADDRESS=8000
export JAVA_OPTS="-Djava.awt.headless=true -Dfile.encoding=UTF-8 -server
-Xms1024m -Xmx2048m -XX:NewSize=512m -XX:MaxNewSize=512m
-XX:PermSize=512m -Dhttp.proxyHost=proxy.cisco.com -Dhttp.proxyPort=80"
export CATALINA_OUT=/dev/null
```

3. CCM または CCO サーバがプロキシをバイパスしてネットワーク リソースに到達する必要がある場合、追加のパラメータが必要になることがあります。

```
-Dhttp.nonProxyHosts=<bypass_hostname>
```

オプション - プロキシをバイパスする /usr/local/tomcat/bin/setenv.sh の例

```
export LD_LIBRARY_PATH=/usr/local/apr/lib
export CATALINA_PID=$CATALINA_HOME/catalina.pid
export JPDA_ADDRESS=8000
export JAVA_OPTS="-Djava.awt.headless=true -Dfile.encoding=UTF-8 -server
-Xms1024m -Xmx2048m -XX:NewSize=512m -XX:MaxNewSize=512m
-XX:PermSize=512m -Dhttp.proxyHost=proxy.cisco.com -Dhttp.proxyPort=80
-Dhttp.nonProxyHosts=10.1.1.1"
export CATALINA_OUT=/dev/null
```

4. Tomcat サービスを再起動します。

```
/etc/init.d/tomcat stop
/etc/init.d/tomcat start
```

5. **ps aux | grep java** コマンドを発行することによって、プロキシ設定が有効であることを確認します。

ps aux | grep java コマンドの出力

```
cliqrus+ 25106 0.0 45.3 4368868 929000 ? Sl Mar02 54:15
/usr/lib/jvm/java-8-sun/bin/java
-Djava.util.logging.config.file=/usr/local/tomcatgua/conf/logging.propert
ies -Djava.util.logging.manager=org.apache.juli.ClassLoaderLogManager
-Djava.awt.headless=true -Dfile.encoding=UTF-8 -server -Xms1024m
-Xmx2048m -XX:NewSize=512m -XX:MaxNewSize=512m -XX:PermSize=512m
-XX:MaxPermSize=512m -Djav.endorsed.dirs=/usr/local/tomcatgua/endorsed
-classpath
/usr/local/tomcatgua/bin/bootstrap.jar:/usr/local/tomcatgua/bin/tomcat-ju
li.jar -Dcatalina.base=/usr/local/tomcatgua
-Dcatalina.home=/usr/local/tomcatgua
-Djava.io.tmpdir=/usr/local/tomcatgua/temp
-Dhttp.proxyHost=proxy.cisco.com -Dhttp.proxyPort=80
-Dhttp.nonProxyHosts=10.1.1.1 org.apache.catalina.startup.Bootstrap start
```

出力に、**-Dhttp.proxyHost=proxy.cisco.com -Dhttp.proxyPort=80 -Dhttp.nonProxyHosts=10.1.1.1** の行が存在することを確認します。

MGMTPOSTGRES：CCM_SA からの DB アクセスの設定

MGMTPOSTGRES に対する CCM_SA からのデータベース アクセスを設定するには、次の手順に従います。

1. CCM ウィザードを起動するには、次のプロセスに従います。
   a. CCM インスタンスに *centos* ユーザとして SSH 接続します。
   b. 次のコマンドを実行します。

```
sudo -i
```

2. CCM ウィザードを呼び出し、CCM_SA へのデータベース アクセスを有効にするように CCM IP を設定します。

CCM ウィザードのパス

```
/usr/local/cliqr/bin/db_config_wizard
```

3. PostgreSQL データベース アクセスを設定するために、CCM IP フィールドに *CCM_SA_IP* を入力します。
4. 変更を確認し、CCM 設定ウィザードを終了します。

CCM（必須）に戻る

CCM ウィザードのプロパティの設定

CCM ウィザードのプロパティを設定するには、次の手順に従います。

1. CCM ウィザードを起動するには、次のプロセスに従います。

a. CCM インスタンスに *CentOS* ユーザとして SSH 接続します。
b. 次のコマンドを実行します。

```
sudo -i
```

2. CCM ウィザードを起動します。

CCM ウィザードのパス

```
/usr/local/cliqr/bin/ccm_config_wizard.sh
```

サーバのプロパティを設定します。

今後の参照のためにこれを書き留めてください。
後で使用できるように、「*インストール方法*」>「*メモ*」セクションを印刷したものにフィールドの詳細を書き留めてください。

ウィザード メニュー	フィールド	説明
メール（Mail） メール通知を送信する SMTP サーバの詳細。デフォルト設定を保持する場合、SMTP サーバの詳細は設定しません。	SMTP ホスト（SMTP Host）	smtp.gmail.com
	SMTP ポート（SMTP Port）	デフォルトは 465 です
	SMTP 認証（SMTP Auth）	ブール値の設定 • True = SMTP サーバでは認証が必要です。 • False = SMTP サーバでは認証が必要ありません。
Mail_User メール通知を送信するメール認証と設定の詳細。デフォルト設定を保持する場合、メール機能は設定せず、電子メールは送信されません。	メール ユーザ（Mail User）	SMTP サーバの電子メールアドレス
	パスワード（Password）	SMTP サーバへのログイン パスワード
	ユーザから（From User）	CCM サーバから電子メールを送信する電子メールアドレス（返信なし）
	表示名（Display Name）	CCM サーバから電子メールを送信するときに表示される名前
Server_info（必須）	パブリック DNS（Public DNS）	CCM の DNS（または IP アドレス）：CCM VM との通信に CCO VM によって使用されます。
	モニタ URL（Monitor URL）	モニタ VM の完全な URL。例：https://<MON IP address>:8443 • HTTPS プロトコルが必要です。 • モニタ VM からのヘルス ステータスの取得に CCM VM で使用されます。
	Hazelcast IP	CCM VM のプライベート IP アドレス：CloudCenter プラットフォームによって内部で使用されます。HA モードでは必要です。
	外部 URL（External URL）	CCM サーバの CloudCenter 外部 URL。HA モードでは必要です。

Config_App_Logo アプリケーション プロファイル テンプレートで使用されます。	DB パスワード（Password）	CCM 非 HA アプライアンス モードでは、PostgreSQL データベースから自動的にこの情報を抽出します。 CCM HA アプライアンス モードではデータベースとしてこの情報を持たないため、相互に通信するためには CCM を両方設定する必要があります。そのため、データベース情報を提供することによってデータベースにアプリケーション プロファイル テンプレートの場所を明示的に設定する必要があります。 デフォルトの DB パスワード = *cliqr* 初回ログイン後は、すぐにこのデフォルト パスワードを変更してください。詳細については、「PostgreSQL Password」を参照してください。
ESB_Info Enterprise Service Bus（ESB）、CloudCenter アプライアンスにデフォルトではインストールされないオプション コンポーネントをインストールした場合にのみ必要。	Rabbit ホスト	ESB AMQP サーバの IP アドレスまたはホスト名です。
	Rabbit ポート	5671
	[管理サーバ アドレス（Management Server Address）]	CCM サーバの IP アドレスまたはホスト名です。
	通知サーバ アドレス（Notification Server Address）	通知サーバの IP アドレスまたはホスト名です（CCM サーバと同じが理想）。
	信頼ストアのパスワード（Trust Store Password）	ESB インスタンスの信頼ストアのパスワードです。
	キー ストアのパスワード（Key Store Password）	ESB インスタンスのキー ストアのパスワード。
ネットワーク（Network）	ホストネーム（Hostname）	CCM サーバのホスト名：変更を行わない場合は、デフォルトを使用します。
DB	IP またはホスト名（IP or Hostname）	データベースの DNS または IP です。 • ローカル ホスト：デフォルト、flyway 移行設定は含まれません • リモート ホスト、flyway 移行設定が含まれます。この行の最後の項目を参照してください。
	[ユーザ名（Username）]	データベース（ローカルまたはリモート）の認証済みユーザ名。
	パスワード（Password）	データベース（ローカルまたはリモート）の認証済みパスワード。
	Flyway 移行（Flyway Migrate）	これはオプションです。リモート ホストは、リモート データベースの IP アドレスを提供することによって、リモート データベースに CCM を設定します。IP アドレスを提供すると、flyway 移行プロセスを設定するための追加の画面が表示されます。 • はい（Yes）：Flyway 移行が行われます。 • いいえ（No）：コンフィギュレーション ファイルのみが更新されます。 DB の設定は、スタンドアロン データベースの導入に必要です。
ELK_Info	ELK ホスト（ELK Host）	ELK ホスト（モニタ VM）の IP アドレスを指定します。
	Elasticsearch ポート（Elasticsearch Port）	8881 がデフォルトで表示されます。
	Logstash ポート（Logstash Port）	4560 がデフォルトで表示されます。
	Kibana ポート（Kibana Port）	8882 がデフォルトで表示されます。

	ELK ユーザ（ELK User）	デフォルトの ELK ユーザ名 = *logreader* です。
	ELK パスワード（Password）	デフォルトの ELK パスワードは *re@d0nly* です（d と n の間は *ゼロ*です）（このパスワードは初回ログイン後に変更してください。詳細については、「Download Log File」を参照してください）。
	ホスト識別子（Host Identifier）	サーバの一意の ID：固有識別子の前に必ず、**CCM_** を追加してください（CCM_1 など）
	ホスト識別子のリスト（Host Identifier List）	HA モードを使用する環境にのみ適用：HA セットアップのすべての ELK/モニタ ホストに対してカンマ区切りの一意のホスト識別子のリストを提供します（例：CCM_1,CCM_2,myCCM）。 HA モードで動作する環境では、それぞれの server.properties ファイルに CCM_1,CCM_2 として固有 ID が設定されている 2 つの CCM インスタンスがある場合、このプロパティは両方の CCM インスタンスで **CCM_1,CCM_2** と示す必要があります。各 CCM は HA モードの他の CCM の固有 ID を認識する必要があります。
Config_Certs：カスタム証明書メニュー	証明書の生成（Generate Certs）	• CloudCenter ID：この CloudCenter の導入を識別するために顧客に割り当てられた一意の英数字文字列。 • 会社名（Company Name）：この証明書が生成される会社の名前。
	証明書の更新（Update Certs）	証明書 Zip パス（Certs Zip Path）：certs.zip ファイルのパスを指定します。デフォルト パスは /tmp/certs.zip です。

3. CCM 設定ウィザードを終了します。
4. Tomcat Service を再起動して変更を適用するには、[はい（Yes）] を選択します。

CCM インスタンスは正常にインストールされました。*これで、次のステップに進むことができます。*

- ヘルス モニタ コンポーネントをインストールしている場合、「*ヘルス モニタ インストール*」を参照してください
- ヘルス モニタ コンポーネントをインストールしていない場合は、「*CloudCenter リージョンごとのインストール*」セクションにスキップし、クラウドごとの CloudCenter コンポーネントのインストールを続行します。

- CCM HA

アプライアンスを使用する CCM HA のインストール

- プロキシの設定
- MGMTPOSTGRES SSH キーの交換
- MGMTPOSTGRES_MASTER – 高可用性プロパティの設定
- CCM_SA_PRIMARY/SECONDARY – CCM SSH キーの交換
- CCM_SA_PRIMARY - HA ウィザードのプロパティの設定
- CCM_LB

CCM HA のインストールは、*AWS*、*OpenStack*、*および VMware* のクラウドでテストおよび検証されています。

HA モードで CCM を設定するには、次のロールを使用する必要があります。

- **データベース**：MGMTPOSTGRES_MASTER と MGMTPOSTGRES_SLAVE（および必要に応じて MGMTPOSTGRES_VIP）
- **CCM**：CCM_SA_PRIMARY と CCM_SA_SECONDARY

  CCM または CCM_SA ロールは使用しないでください。これらのロールでは、高可用性を設定できません。詳細については、「仮想アプライアンスの概要」と「高可用性のベスト プラクティス」を参照してください。

- **ロードバランサ**：CCM_LB

プロキシの設定

インターネットへの接続にプロキシ サーバが必要な場合は、CCM と CCO サーバのプロキシ設定で Tomcat Service を設定していることを確認してください。

プロキシ サーバを使用してインターネットに接続するには、次の手順を実行します。

1. プロキシ設定を反映するようにプロキシ環境を変更します。
2. /usr/local/tomcat/bin/setenv.sh ファイルでは、既存の **JAVA_OPTS** 環境変数に次のパラメータを追加することが CloudCenter プラットフォームにより要求されます。

HTTP の場合に必須 - JAVA_OPTS 環境変数に次のパラメータを追加します

```
-Dhttp.proxyHost=<proxy_hostname> -Dhttp.proxyPort=<port_number>
```

または

HTTPS の場合に必須 - JAVA_OPTS 環境変数に次のパラメータを追加します

```
-Dhttps.proxyHost=<proxy_hostname> -Dhttps.proxyPort=<port_number>
```

JAVA_OPTS にパラメータが追加された /usr/local/tomcat/bin/setenv.sh の例

```
export LD_LIBRARY_PATH=/usr/local/apr/lib
export CATALINA_PID=$CATALINA_HOME/catalina.pid
export JPDA_ADDRESS=8000
export JAVA_OPTS="-Djava.awt.headless=true -Dfile.encoding=UTF-8 -server
-Xms1024m -Xmx2048m -XX:NewSize=512m -XX:MaxNewSize=512m
-XX:PermSize=512m -Dhttp.proxyHost=proxy.cisco.com -
Dhttp.proxyPort=80" export CATALINA_OUT=/dev/null
```

3. CCM または CCO サーバがプロキシをバイパスしてネットワーク リソースに到達する必要がある場合、追加のパラメータが必要になることがあります。

```
-Dhttp.nonProxyHosts=<bypass_hostname>
```

オプション - プロキシをバイパスする /usr/local/tomcat/bin/setenv.sh の例

```
export LD_LIBRARY_PATH=/usr/local/apr/lib
export CATALINA_PID=$CATALINA_HOME/catalina.pid
export JPDA_ADDRESS=8000
export JAVA_OPTS="-Djava.awt.headless=true -Dfile.encoding=UTF-8 -server
-Xms1024m -Xmx2048m -XX:NewSize=512m -XX:MaxNewSize=512m
-XX:PermSize=512m -Dhttp.proxyHost=proxy.cisco.com -Dhttp.proxyPort=80
-Dhttp.nonProxyHosts=10.1.1.1"
export CATALINA_OUT=/dev/null
```

4. Tomcat サービスを再起動します。

```
/etc/init.d/tomcat stop
/etc/init.d/tomcat start
```

5. **ps aux | grep java** コマンドを発行することによって、プロキシ設定が有効であることを確認します。

ps aux | grep java コマンドの出力

```
cliqrus+ 25106 0.0 45.3 4368868 929000 ? Sl Mar02 54:15
/usr/lib/jvm/java-8-sun/bin/java
-Djava.util.logging.config.file=/usr/local/tomcatgua/conf/logging.propert
ies -Djava.util.logging.manager=org.apache.juli.ClassLoaderLogManager
-Djava.awt.headless=true -Dfile.encoding=UTF-8 -server -Xms1024m
-Xmx2048m -XX:NewSize=512m -XX:MaxNewSize=512m -XX:PermSize=512m
-XX:MaxPermSize=512m -Djav.endorsed.dirs=/usr/local/tomcatgua/endorsed
-classpath
/usr/local/tomcatgua/bin/bootstrap.jar:/usr/local/tomcatgua/bin/tomcat-
ju li.jar -Dcatalina.base=/usr/local/tomcatgua
-Dcatalina.home=/usr/local/tomcatgua
-Djava.io.tmpdir=/usr/local/tomcatgua/temp
-Dhttp.proxyHost=proxy.cisco.com -Dhttp.proxyPort=80
-Dhttp.nonProxyHosts=10.1.1.1 org.apache.catalina.startup.Bootstrap start
```

出力に、**-Dhttp.proxyHost=proxy.cisco.com -Dhttp.proxyPort=80 -Dhttp.nonProxyHosts=10.1.1.1** の行が存在することを確認します。

MGMTPOSTGRES SSH キーの交換

MGMTPOSTGRES_MASTER と MGMTPOSTGRES_SLAVE の間で SSH キーを交換するには、次の手順に従います。

1. MGMTPOSTGRES_MASTER で、新しい SSH キーを生成するには、次のコマンドを実行します。

```
sudo -i

#The ssh-keygen -t rsa command has two options (use the defaults by
pressing enter or providing a custom name -- CAUTION: Do NOT provide a
custom name at this point and continue by using the defaults).

ssh-keygen -t rsa

cd ~/.ssh
cat id_rsa.pub >> authorized_keys
```

2. MGMTPOSTGRES_SLAVE に **.ssh ディレクトリがない場合**は、ファイルをコピーする前に、次のコマンドを使用して作成します。

```
sudo -i
mkdir -p ~/.ssh
chmod 700 ~/.ssh
```

3. MGMTPOSTGRES_MASTER から MGMTPOSTGRES_SLAVE の同じ場所に id_rsa ファイル（~/.ssh/id_rsa と ~/.ssh/id_rsa.pub）をコピーします。

```
#MGMTPOSTGRES_MASTER command:
cat ~/.ssh/id_rsa

#Content of this file displays...copy the content.

#MGMTPOSTGRES_SLAVE command:
vi ~/.ssh/id_rsa

#Paste the copied content here, delete blank lines, and save the file
```

4. MGMTPOSTGRES_SLAVE で、次のコマンドを実行し、新しい SSH キーを生成します。

```
sudo -i
chmod 400 ~/.ssh/id_rsa*

cd ~/.ssh
cat id_rsa.pub >> authorized_keys
```

5. 各 VM 上で次のコマンドを実行して、MGMTPOSTGRES_MASTER と MGMTPOSTGRES_SLAVE 間の相互 SSH アクセスを確認します。

```
sudo -i
ssh root@<MGMTPOSTGRES_MASTER/MGMTPOSTGRES_SLAVE>
```

CCM（必須）に戻る

MGMTPOSTGRES_MASTER – 高可用性プロパティの設定

MGMTPOSTGRES_MASTER の高可用性を設定するには、次の手順に従います。

1. DB ウィザードを起動するには、次のプロセスに従います。
   a. DB インスタンスに *centos* ユーザとして SSH 接続します。
   b. 次のコマンドを実行します。

```
sudo -i
```

2. ウィザードを起動します。

MGMTPOSTGRES ウィザードのパス
/usr/local/cliqr/bin/db_config_wizard.sh

3. PostgreSQL データベースの HA を確保するように Postgres HA を設定し、次のように各フィールドに情報を入力します。

> **今後の参照のためにこれを書き留めてください。**
> 後で使用できるように、「*インストール方法*」>「*メモ*」セクションを印刷したものにフィールドの詳細を書き留めてください。

その他の設定については、「Configure CCM Wizard Properties」を参照してください。

ウィザード メニュー	フィールド	説明
Configure_Postgres_HA	DB マスター（DB Master）	マスター データベース VM のホスト名 - 構成できません。
	DB マスター プライベート IP（DB Master Private IP）	マスター データベース VM のプライベート IP アドレス
	DB スレーブ ホスト名（DB Slave Hostname）	マスター データベース VM のホスト名
	DB スレーブ プライベート IP（DB Slave Private IP）	スレーブ データベース VM のプライベート IP アドレス
	VIP *または* EIP	データベースの VIP/EIP IP このオプションを選択するには、マウスを使用します。 EIP の AWS クラウドの微妙な違い SA または HA モードで RDS サービスとして PostgreSQL をセットアップするには、「*Confi guring HA for PostgreSQL Database on AWS*」を参照してください。

詳細を入力すると、データベース サーバは、HA 設定に続いてデータベース サーバ間のレプリケーション設定を開始し、最終的に次のステータス メッセージが表示されます。

- データベースの HA を設定中...（Configuring database for HA ...）
- データベースのレプリケーションを設定中（Configuring database for replication）

4. 設定ウィザードを終了します。
5. 各 PostgreSQL サーバのコマンド ラインに移動し、次のコマンドを入力して、データベースと HA 接続の状態を確認します。
   # **pcs status**
   a. 両方のデータベース サーバの [PCSD ステータス（PCSD Status）] が [オンライン（Online）] であることを確認します。
   b. Corosync、Pacemaker、および pcsd サービスの [デーモン ステータス（Daemon Status）] が [アクティブ/無効（active/disabled）] であることを確認します。

CCM（必須）に戻る

CCM_SA_PRIMARY/SECONDARY – CCM SSH キーの交換

CCM_SA_PRIMARY と CCM_SA_SECONDARY サーバ間で SSH キーを交換するには、次の手順に従います。

1. CCM_SA_PRIMARY で、新しい SSH キーを生成するには、次のコマンドを実行します。

```
su - cliqruser
ssh-keygen -t rsa
cd ~/.ssh
cat id_rsa.pub >> authorized_keys
```

2. CCM_SA_PRIMARY から CCM_SA_SECONDARY の同じ場所に id_rsa ファイル（~/.ssh/id_rsa と ~/.ssh/id_rsa.pub）をコピーします。CCM_SA_SECONDARY に .ssh ディレクトリがない場合は、ファイルをコピーする前に、次のコマンドを使用して作成します。

```
su - cliqruser
mkdir -p ~/.ssh
chmod 700 ~/.ssh
```

3. CCM_SA_SECONDARY で、次のコマンドを実行し、新しい SSH キーを追加します。

```
su - cliqruser
chmod 400 ~/.ssh/id_rsa*
cat id_rsa.pub >> authorized_keys
chmod 600 authorized_keys
```

4. 各 VM 上で次のコマンドを実行して、CCM_SA_PRIMARY と CCM_SA_SECONDARY 間の相互 SSH アクセスを確認します。

```
su - cliqruser
ssh cliqruser@<CCM_SA_PRIMARY/CCM_SA_SECONDARY>
```

CCM_SA_PRIMARY - HA ウィザードのプロパティの設定

CCM_SA_PRIMARY の高可用性を設定するには、次の手順に従います。

1. CCM ウィザードを起動するには、次のプロセスに従います。
   a. CCM インスタンスに *centos* ユーザとして SSH 接続します。
   b. 次のコマンドを実行します。

```
sudo -i
```

2. CCM ウィザードを起動します。

CCM ウィザードのパス

```
/usr/local/cliqr/bin/ccm_config_wizard.sh
```

プロパティを設定します。

> **今後の参照のためにこれを書き留めてください。**
> 後で使用できるように、「*インストール方法*」>「*メモ*」セクションを印刷したものにフィールドの詳細を書き留めてください。

ウィザード メニュー	フィールド	説明
[DB – DB の入力（DB – Enter DB）] パラメータ	マスター プライベート IP および スレーブ プライベート IP（Master Private IP and Slave Private IP）	マスター データベースとスレーブ データベースの VIP/EIP。詳細については、「*フェーズ 1: インフラストラクチャの準備*」>「*クラウドの微妙な違い*」を参照してください。 「MGMTPOSTGRES_MASTER – 高可用性プロパティの設定」の設定を行うと、`db _config_wizard` の VIP/EIP アドレスは設定済みになります。同様に、CCM_SA_PRIMARY と CCM_SA_SECONDARY サーバの EIP/VIP アドレスを指定する必要があります。
	DB ユーザ名および DB パスワード（DB Username and DB Password）	次のクレデンシャルは、あらかじめ設定されています。 デフォルト ユーザ名 = *cliqr*（変更不可） デフォルト パスワード = cliqr（変更可能） 初回ログイン後は、すぐにこのデフォルト パスワードを変更してください。詳細については、「Po stgreSQL Password」を参照してください。
Configure_HA	プライマリ ノード プライベート IP（Primary Node Private IP）	プライマリ CCM VM の IP アドレス
	セカンダリ ノード プライベート IP（Secondary Node Private IP）	セカンダリ CCM VM の IP アドレス
	パブリック DNS（Public DNS）	CCM_LB の DNS または IP を使用 - CCM VM との通信に CCO VM によって使用されます。

	Hazelcast IP	カンマで区切られた、プライマリおよびセカンダリ CCM VM のパブリックまたはプライベート IP アドレスである必要があります。2 つの CCM VM の設定先: • 同じネットワーク上の場合、プライベート IP アドレスを使用します。 • 異なるネットワーク上の場合、パブリック IP アドレスを使用します。
	外部 URL（External URL）	CCM_LB_IP を使用します。 • 非 HA CCM シナリオではオプション • HA CCM シナリオでは**必須**

3. 詳細を入力すると、データベース サーバは、HA 設定に続いてデータベース サーバ間のレプリケーション設定を開始し、最終的に次のステータス メッセージが表示されます。
   - CCM HA を設定中...（Configuring CCM HA ...）
   - 「サーバの再起動（Restart server）」（経過表示バー）
   - CCM HA の設定に成功しました（Configured CCM HA successfully）

   CCM プライマリ サーバに HA を設定した後、次のメッセージが表示されます。
   cliqruser に sudo 権限がないため、セカンダリ CCM tomcat を再起動できませんでした。（Restarting secondary ccm tomcat failed due to cliqruser may not have sudo permission.）

   この時点で、セカンダリ CCM サーバの tomcat を手動で再起動する必要があります。
4. CCM セカンダリ サーバで次のコマンドを実行して、Tomcat サーバを再起動します。

```
sudo -i
/etc/init.d/tomcat restart
```

5. CCM 設定ウィザードを終了します。

CCM_LB

導入のためにオープンにする必要があるポートの完全なリストについては、「CCM ファイアウォール ルール」>「*CCM_LB ポート*」を参照してください。

CloudCenter コンポーネントのロード バランサを設定する場合は、firewalld がデフォルトで有効になっていることに注意してください。CloudCenter コンポーネントがロード バランサと通信できるようにするには、明示的に無効にする必要があります。詳細については、「ファイアウォール ルールの概要」を参照してください。

CCM の HAProxy で CentOS7.x VM をロード バランシングする設定例です。

1. VM を起動するために使用するキー ペアを使用して VM インスタンスに SSH 接続します。
2. ルート ユーザとして HAProxy をインストールします。

```
yum install -y haproxy
```

3. CCM プライマリ サーバで CCM_LB の haproxy 設定の .pem ファイルを作成します。
   a. 次のコマンドを実行します。

```
sudo -i
cd /usr/local/tomcat/conf/ssl
cat mgmtserver.crt mgmtserver.key >> mgmtserver.pem
cat ca.crt mgmtserver.key >> ca.pem
```

   環境に応じて mgmtserver および ca pem に名前を付けることができますが、.pem 拡張子を必ず追加してください。

b. 以前に CCM_LB サーバに作成した mgmtserver.pem および ca.pem ファイルを /etc/haproxy の場所に置きます。

4. HAProxy の設定ファイルに次の詳細情報を追加します。

```
vi /etc/haproxy/haproxy.cfg

# configuration to listen on 443 with SSL certs and loadbalance
frontend https-in
    mode http
    log global
    bind *:443 ssl crt /etc/haproxy/mgmtserver.pem ca-file
/etc/haproxy/ca.pem
    default_backend ccms

# configuration to listen on 8443 with SSL certs and loadbalance
frontend httpsalt-in
    mode tcp
    bind *:8443
    default_backend nodes

backend ccms
    balance roundrobin
    mode    http
    log global
    option httplog
    cookie SVR insert preserve nocache
    server  ccm1 <CCM_SA_PRIMARY_IP>:443 check cookie ccm1 ssl verify
none
    server  ccm2 <CCM_SA_SECONDARY_IP>:443 check cookie ccm2 ssl verify
none

backend nodes
    mode tcp
    balance roundrobin
    option ssl-hello-chk
    server  ccm1 <CCM_SA_PRIMARY_IP>:8443 check
    server  ccm2 <CCM_SA_SECONDARY_IP>:8443 check
```

5. HAProxy サービスを開始し、ステータス応答がアクティブであることを確認します。

```
systemctl start haproxy
systemctl status haproxy
```

6. この時点では、HTTPS を使用して CCM サーバを呼び出す必要があります。次に例を示します。

```
https://myCCM_LB_server.com

#or

https://<CCM_LB_IP_Address>
```

CCM（必須）に戻る

アプライアンスを使用するモニタのインストール（必須）

Elasticsearch、Logstash、Kibana は *ELK スタック*と総称され、ヘルス モニタをインストールするとデフォルトでインストールされます。ログ ファイルをダウンロードできるようにするには、このコンポーネントを必ずインストールしてください。

モニタ ウィザードのプロパティの設定

モニタは、CloudCenter の必須コンポーネントです。

1. MONITOR ウィザードを起動するには、次のプロセスに従います。
   a. MONITOR インスタンスに *centos* ユーザとして SSH 接続します。
   b. 次のコマンドを実行します。

```
sudo -i
```

2. ウィザードを起動します。

モニタ ウィザード パス
/usr/local/cliqr/bin/monitor_config_wizard.sh

3. モニタ インスタンスのプロパティを設定します。

今後の参照のためにこれを書き留めてください。
後で使用できるように、「*インストール方法*」>「*メモ*」セクションを印刷したものにフィールドの詳細を書き留めてください。

ウィザード メニュー	フィールド	注記（Notes）
CCM_Info	Monitor ID	ヘルス チェック インスタンスに使用される一意の（英数字）識別子。
	CCM [ホスト名/URL（Hostname/URL）]（必須）	• CCM_IP または • CCM_SA_IP または • CCM_LB_IP
	Monitor User	クラウド リージョンのヘルス チェックを有効にするために CCM サーバで設定されたユーザ ID。 • 有効化されたすべてのクラウド リージョンでヘルス チェックを実行するには、この値を 2 に設定します（2 は CloudCenter のルート管理者のユーザ ID です）。 • 特定のクラウド リージョンでヘルスチェックを実行する場合は、それらのリージョンを使用して新しいユーザを作成してアクティブ化し、そのユーザのユーザ ID をこのプロパティの値として使用します。ユーザ ID を取得するには、v1 ユーザ管理 API を使用します。
ELK_Login	ELK ユーザ（ELK User）	ELK/モニタ ホストのデフォルト ユーザ名は ***logreader* です。**
	ELK パスワード（ELK Password）	デフォルトの ELK パスワードは ***re@d0nly*** です（d と n の間は*ゼロ*です）（このパスワードは初回ログイン後に変更してください。詳細については、「Download Log Files」を参照してください）。
Config_Certs	証明書 Zip パス（Certs Zip Path）	certs.zip ファイルのパスを指定します。デフォルト パスは /tmp/certs.zip です。

4. 変更を確認し、モニタ設定ウィザードを終了します。
5. Tomcat Service を再起動して変更を適用するには、[はい（Yes）] を選択します。

モニタ インスタンスは正常に設定されました。「*CloudCenter リージョンごとのインストール*」セクションに進み、各クラウドの CloudCenter コンポーネントをインストールできます。

*CCM（必須）*および *CCO（必須）*サーバで ELK スタックとのモニタの詳細を設定したことを確認してください。

仮想アプライアンスを使用するリポジトリのインストール

- リポジトリ仮想アプライアンス
- リポジトリ ウィザードのプロパティの設定

リポジトリ仮想アプライアンス

リポジトリ仮想アプライアンスには、複数のソフトウェア パッケージと、CloudCenter パッケージが使用するより小さなコンポーネント（サービス バンドル、ソフトウェア パッケージ、バイナリ、スクリプト、Docker イメージなど）の仮想アプライアンスが含まれます。リポジトリ仮想アプライアンスをインストールして設定すると、含まれるコンポーネントがインストールされ、関連付けられているプロパティは、CCM ウィザード、CCO ウィザード、または AMQP ウィザードで必要な場合に設定できます。

このリポジトリ アプライアンス：

- CentOS7 サーバ上で Nginx を使用します。
- CloudCenter の各リリースに固有のバージョンです。

リポジトリ モード	役割	タイプ（Type）	目的
非 HA	REPO	VM	サービス バンドル、パッケージ ストア、スクリプトなどのため

リポジトリ ウィザードのプロパティの設定

リポジトリ（repo）ウィザードのプロパティを設定するには、次の手順に従います。

1. リポジトリ ウィザードを起動するには、次のプロセスに従います。
   a. リポジトリ インスタンスに *CentOS* ユーザとして SSH 接続します。
   b. 次のコマンドを実行します。

```
sudo -i
```

   c. リポジトリ ウィザードを起動します。

CCM ウィザードのパス

```
/usr/bin/repo_config_wizard.sh.
```

   d. サーバのプロパティを設定します。

今後の参照のためにこれを書き留めてください。
後で使用できるように、「*インストール方法*」>「*メモ*」セクションを印刷したものにフィールドの詳細を書き留めてください。

ウィザード メニュー	フィールド	説明
パッケージ ストア	マスターの変更（Change Master）	**リポジトリの URL**： 同期するこのリポジトリのマスター リポジトリを設定します。 デフォルトのマスターは repo.cliqrtech.com です。URL を別のマスター リポジトリに変更するには、そのリポジトリの URL を指定します。
	Set_Master	ローカル リポジトリをマスター リポジトリに変更します。ローカル リポジトリはマスター リポジトリと同期されなくなります。このオプションを選択する場合、リポジトリの詳細（パッケージの更新、イメージ xml の更新など）を指定して保持する必要があります。
	Repo_Syncup	マスター リポジトリと同期し、マスター リポジトリからのすべての変更（ある場合）を更新します。
	Add_ssh_key	このリポジトリをマスター リポジトリとして使用する場合は、このオプションを使用して、このリポジトリを指すローカルリポジトリに SSH キーを追加します。

バンドル ストア – Set_Bundle_URL	バンドル フォルダ（Bundle Folder）	バンドル ストアのフォルダ バージョンを更新します。 repo/bundle/*CloudCenter_Version* 例： repo/bundle/4.8.0

	バンドル URL（Bundle URL）	バンドル ストアの URL を更新します。
		`http://your_HTTP_server/bundle/release-CloudCenter_Version/`
		例：
		`http://repo.cliqrtech.com/bundle/release-4.8.0/`
		⚠ コマンドの末尾に「/」を含めないと、プロセスのどこかの時点でエラーが発生します。
		ⓘ 各リリースの正しいパスを検証するため、任意のブラウザでバンドル URL を入力し、ファイルがダウンロードされたことを確認します。
		バンドル ストア ファイルが CloudCenter プラットフォームに利用できます。
		✓ http://*your_HTTP_server*/bundle/release-*CloudCenter_Version/* パスを将来変更する場合は、必ず release-*CloudCenter_Version/* フォルダ レベルまでのパスを指定してください。
		✓ 前に指定されたフォルダ構造を使用してください。パスはコンポーネントによって異なります。

2. リポジトリ ウィザードを終了します。
3. リポジトリ インスタンスは正常にインストールされました。

「クラウド リージョンごと（必須）」に進むことができます。専用のパッケージ ストア、バンドル ストア、または Docker レジストリを設定している場合は、CCO ウィザードでリポジトリ固有の URL を指定してください。

クラウド リージョンごとのインストール（必須）

- AMQP（必須）

アプライアンスを使用する AMQP のインストール

AMQP 非 HA

AMQP 非 HA

- AMQP - Guacamole サーバの CCM/CCO プロパティの設定
- AMQP の再起動

ⓘ このコンポーネントは、クラウド リージョンごと（パブリック クラウド、プライベート クラウド、またはデータセンター）に必要です。

⚠ **専用 Gucamole のセットアップ**
この GUA 設定ウィザードの手順は、専用の Guacamole サーバ（オプション）をセットアップしている場合は必須ではありません。自己署名 Guacamole 証明書は、アプライアンスのインストール用にすぐに使用できるよう提供されます。

AMQP - Guacamole サーバの CCM/CCO プロパティの設定

AMQP プライマリ サーバと AMQP セカンダリ サーバの両方で次の gua_config_wizard.sh プロシージャを設定します。

1. GUA ウィザードを起動するには、次のプロセスに従います。
   a. GUA インスタンスに *centos* ユーザとして SSH 接続します。
   b. 次のコマンドを実行します。

```
sudo -i
```

2. GUA ウィザードを起動します。

GUA ウィザードのパス
/usr/local/cliqr/bin/gua_config_wizard.sh

3. CCM と CCO（インストール後）のプロパティを設定します。

今後の参照のためにこれを書き留めてください。
後で使用できるように、「*インストール方法*」>「*メモ*」セクションを印刷したものにフィールドの詳細を書き留めてください。

4. CCM および CCO（インストール後）の VM のプロパティを設定します。

ウィザード メニュー	フィールド	使用可能な IP アドレス
CCM_Info	CCM ホスト（CCM Host）	*CCM_IP* または *CCM_SA_IP* または *CCM_LB_IP*
CCO_Info	CCO ホスト（CCO Host）（インストール後）	*CCO_IP* または *CCO_LB_IP*
Config_Certs	証明書 Zip パス（Certs Zip Path）	certs.zip ファイルのパスを指定します。デフォルト パスは /tmp/certs.zip です。

5. 変更を確認し、GUA 設定ウィザードを終了します。
6. Tomcat Service を再起動して変更を適用するには、[はい（Yes）] を選択します。

初めて AMQP インスタンスをインストールする場合は、すべてのユーザが表示されていることを確認するまで数分待つ必要があることがあります。次のコマンドを実行して、すべてのユーザが表示されていることを確認できます。

```
root> ls -alrt /usr/local/osmosix/etc/.RABBITINSTALLED
-rw-r--r--. 1 root root o Feb 17 23:07
/user/local/osmosix/etc/.RABBITINSTALLED
root> rabbitmqctl list_users
Listing users ...
cliqr     [administrator]
cliqr_worker       []
guest     [administrator]
root>
```

AMQP の再起動

AMQP VM の再起動
AMQP サーバのホスト名を変更する場合、ローカル AMQP データベースの名前が変更されるため、AMQP VM を再起動する必要があります。

- AMQP VM を再起動するには、**root** として次のコマンドを実行します。

```
rm /usr/local/osmosix/etc/.RABBITINSTALLED
/usr/local/osmosix/bin/rabbit_config.sh
reboot
```

- VM を再起動する場合は、次の詳細に注意してください。
  - 再起動後、結局、新しいホスト名とデータベース名になることがあります。
  - 一部のクラウドでは、新しいインスタンスまたは再起動に対して自動的にホスト名が設定されます。RabbitMQ は設定済みのホスト名を使用してデータベース名を設定します。
  - データベース ユーザが存在し、ログインが関連付けられていない場合、このユーザは AMQP サーバにログインできない可能性があります。
    - 必要なユーザ（**cliqr** および **cliqr_worker**）がデータベースに設定されていることを確認します。データベースに追加のユーザが設定されている場合は、**rabbitmqctl** コマンドを実行すると表示されます。

```
rabbitmqctl list_users
Listing users ...
cliqr [administrator]
cliqr_worker []
```

    - データベースにこれらのユーザが表示されない場合は、root として次のコマンドを実行します（AMQP 構成でユーザを再作成します）。

```
rm
/usr/local/osmosix/etc/.RABBITINSTALLED
bash
/usr/local/osmosix/bin/rabbit_config.sh
```

AMQP インスタンスは正常に設定されました。「*CCO（必須）*」セクションに進んでください。

AMQP HA

アプライアンスを使用する AMQP HA のインストール

- AMQP_PRIMARY/SECONDARY – AMQP SSH キーの交換
- AMQP - Guacamole サーバの CCM/CCO プロパティの設定
- AMQP の再起動
- AMQP_PRIMARY – 高可用性プロパティの設定
- AMQP_LB

AMQP_PRIMARY/SECONDARY – AMQP SSH キーの交換

AMQP_PRIMARY と AMQP_SECONDARY サーバ間で SSH キーを交換するには、次の手順に従います。

1. AMQP_PRIMARY で、新しい SSH キーを生成するには、（root として）次のコマンドを実行します。

```
sudo -i
ssh-keygen -t rsa
cd ~/.ssh
cat id_rsa.pub >> authorized_keys
```

2. AMQP_PRIMARY から AMQP_SECONDARY の同じ場所に id_rsa ファイル（~/.ssh/id_rsa と ~/.ssh/id_rsa.pub）を（root として）コピーします。AMQP_SECONDARY に .ssh ディレクトリがない場合は、ファイルをコピーする前に、次のコマンドを使用して作成します。

```
sudo -i
mkdir -p ~/.ssh
chmod 700 ~/.ssh
```

3. AMQP_SECONDARY で、新しい SSH キーを生成するには、（root として）次のコマンドを実行します。

```
sudo -i
chmod 400 ~/.ssh/id_rsa*
cat id_rsa.pub >> authorized_keys
chmod 600 authorized_keys
```

4. 各 VM 上で次のコマンドを実行して、AMQP_PRIMARY と AMQP_SECONDARY 間の相互 SSH アクセスを確認します。

```
sudo -i
ssh root@<AMQP_PRIMARY/AMQP_SECONDARY>
```

両方の AMQP インスタンスに SSH が設定されました。

このコンポーネントは、クラウド リージョンごと（パブリック クラウド、プライベート クラウド、またはデータセンター）に必要です。

専用 Gucamole のセットアップ
この GUA 設定ウィザードの手順は、専用の Guacamole サーバ（オプション）をセットアップしている場合は必須ではありません。自己署名 Guacamole 証明書は、アプライアンスのインストール用にすぐに使用できるよう提供されます。

AMQP - Guacamole サーバの CCM/CCO プロパティの設定

AMQP プライマリ サーバと AMQP セカンダリ サーバの両方で次の gua_config_wizard.sh プロシージャを設定します。

1. GUA ウィザードを起動するには、次のプロセスに従います。
   a. GUA インスタンスに *centos* ユーザとして SSH 接続します。
   b. 次のコマンドを実行します。

```
sudo -i
```

2. GUA ウィザードを起動します。

GUA ウィザードのパス
/usr/local/cliqr/bin/gua_config_wizard.sh

3. CCM と CCO（インストール後）のプロパティを設定します。

今後の参照のためにこれを書き留めてください。
後で使用できるように、「*インストール方法*」>「*メモ*」セクションを印刷したものにフィールドの詳細を書き留めてください。

4. CCM および CCO（インストール後）の VM のプロパティを設定します。

ウィザード メニュー	フィールド	使用可能な IP アドレス
CCM_Info	CCM ホスト（CCM Host）	*CCM_IP* または *CCM_SA_IP* または *CCM_LB_IP*
CCO_Info	CCO ホスト（CCO Host）（インストール後）	*CCO_IP* または *CCO_LB_IP*
Config_Certs	証明書 Zip パス（Certs Zip Path）	certs.zip ファイルのパスを指定します。デフォルト パスは /tmp/certs.zip です。

5. 変更を確認し、GUA 設定ウィザードを終了します。
6. Tomcat Service を再起動して変更を適用するには、[はい（Yes）] を選択します。

初めて AMQP インスタンスをインストールする場合は、すべてのユーザが表示されていることを確認するまで数分待つ必要があることがあります。次のコマンドを実行して、すべてのユーザが表示されていることを確認できます。

```
root> ls -alrt /usr/local/osmosix/etc/.RABBITINSTALLED
-rw-r--r--. 1 root root o Feb 17 23:07
/user/local/osmosix/etc/.RABBITINSTALLED
root> rabbitmqctl list_users
Listing users ...
cliqr     [administrator]
cliqr_worker       []
guest     [administrator]
root>
```

AMQP の再起動

AMQP VM の再起動
AMQP サーバのホスト名を変更する場合、ローカル AMQP データベースの名前が変更されるため、AMQP VM を再起動する必要があります。

- AMQP VM を再起動するには、**root** として次のコマンドを実行します。

```
rm /usr/local/osmosix/etc/.RABBITINSTALLED
/usr/local/osmosix/bin/rabbit_config.sh
reboot
```

- VM を再起動する場合は、次の詳細に注意してください。
  - 再起動後、結局、新しいホスト名とデータベース名になることがあります。
  - 一部のクラウドでは、新しいインスタンスまたは再起動に対して自動的にホスト名が設定されます。RabbitMQ は設定済みのホスト名を使用してデータベース名を設定します。
  - データベース ユーザが存在し、ログインが関連付けられていない場合、このユーザは AMQP サーバにログインできない可能性があります。
    - 必要なユーザ（**cliqr** および **cliqr_worker**）がデータベースに設定されていることを確認します。データベースに追加のユーザが設定されている場合は、**rabbitmqctl** コマンドを実行すると表示されます。

```
rabbitmqctl list_users
Listing users ...
cliqr [administrator]
cliqr_worker []
```

    - データベースにこれらのユーザが表示されない場合は、root として次のコマンドを実行します（AMQP 構成でユーザを再作成します）。

```
rm
/usr/local/osmosix/etc/.RABBITINSTALLED
bash
/usr/local/osmosix/bin/rabbit_config.sh
```

AMQP インスタンスは正常に設定されました。「*CCO（必須）*」セクションに進んでください。

AMQP_PRIMARY – 高可用性プロパティの設定

AMQP プライマリ サーバ***のみ***で次の rabbit_config_wizard.sh プロシージャを設定します。

1. AMQP ウィザードを起動するには、次のプロセスに従います。
   a. AMQP インスタンスに *centos* ユーザとして SSH 接続します。
   b. 次のコマンドを実行します。

```
sudo -i
```

2. AMQP ウィザードを起動します。

GUA ウィザードのパス
/usr/local/cliqr/bin/rabbit_config_wizard.sh

3. CCM と CCO（インストール後）のプロパティを設定します。

今後の参照のためにこれを書き留めてください。
後で使用できるように、「*インストール方法*」>「*メモ*」セクションを印刷したものにフィールドの詳細を書き留めてください。

4. CCM および CCO（インストール後）の VM のプロパティを設定します。

ウィザード メニュー	フィールド	使用可能な IP アドレス
Configure_HA	プライマリ ノード IP（Primary Node IP）	*AMQP_PRIMARY* インスタンスの IP アドレス。
	プライマリ ホスト名（Primary Hostname）	*AMQP_PRIMARY* インスタンスのホスト名。
	セカンダリ ノード IP（Secondary Node IP）	*AMQP_SECONDARY* インスタンスの IP アドレス。
	セカンダリ ホスト名（Secondary Hostname）	*AMQP_PRIMARY* インスタンスのホスト名。

5. 変更を確認し、AMQP 設定ウィザードを終了します。
6. Tomcat Service を再起動して変更を適用するには、[はい（Yes）] を選択します。

AMQP インスタンスの高可用性プロパティが正常に設定されました。「*AMQP_LB*」セクションに進んでください。

AMQP_LB

AMQP のロード バランシングは、HAProxy、NGiNX、Apache2、または AWS Elastic ロード バランサ（ELB）などのサービスをネイティブで使用できるクラウドで実行できます。ロード バランサ サービスを設定し、AMQP ロード バランシングを確認するには、ポート 5671 でリスニングし、AMQP_PRIMARY および AMQP_SECONDARY サーバの両方の 443 で要求を調整してください。

導入のためにオープンにする必要があるポートの完全なリストについては、「AMQP ファイアウォール ルール」>「*AMQP_LB ポート*」を参照してください。

> CloudCenter コンポーネントのロード バランサを設定する場合は、firewalld がデフォルトで有効になっていることに注意してください。CloudCenter コンポーネントがロード バランサと通信できるようにするには、明示的に無効にする必要があります。詳細については、「ファイアウォール ルールの概要」を参照してください。

次のロード バランシング設定が AMQP VM の HAProxy と CentOS7.x VM で行われました。

1. VM を起動するために使用するキー ペアを使用して VM インスタンスに SSH 接続します。
2. ルート ユーザとして HAProxy をインストールします。

```
yum install -y haproxy
```

3. 次のように、HAProxy の設定ファイルを変更します

```
vi /etc/haproxy/haproxy.cfg

#configuration to listen on 5671 and loadbalance

frontend amqps-in
    mode tcp
    log global
    bind *:5671
    default_backend amqps
backend amqps
    mode tcp
    balance roundrobin
    option ssl-hello-chk
    server amqp1 <AMQP_PRIMARY>:5671 check
    server amqp2 <AMQP_SECONDARY>:5671 check
#configuration to listen on 443 and loadbalance
frontend gua-in
    mode tcp
    log global
    bind *:443
    default_backend guas
backend guas
   mode tcp
   balance source
   cookie SVR insert preserve nocache
   option ssl-hello-chk
   server amqp1 <AMQP_PRIMARY>:443 check
   server amqp2 <AMQP_SECONDARY>:443 check
```

4. 5671 ポートにバインドするには、SELinux を無効にする必要があります（SELinux を無効にするには次のコマンドを実行します）。

```
setenforce 0
sed -i 's/=enforcing/=permissive/g' /etc/selinux/config*
#This command ensures that SELINUX is disabled permanently and
the changes are retained even in case of reboot
```

5. HAProxy サービスを開始し、そのステータスを確認します。これはアクティブである必要があります

```
systemctl start haproxy
systemctl status haproxy
```

AMQP インスタンスは正常に設定されました。「*CCO（必須）*」セクションに進んでください。

- CCO（必須）

アプライアンスを使用する CCO のインストール（必須）

CCO 非 HA

CCO ウィザードのプロパティの設定

このコンポーネントは、クラウド リージョンごと（パブリック クラウド、プライベート クラウド、またはデータセンター）に必要です。

1. CCO ウィザードを起動するには、次のプロセスに従います。
   a. CCO インスタンスに *centos* ユーザとして SSH 接続します。
   b. 次のコマンドを実行します。

```
sudo -i
```

- CCO ウィザードを起動します。

CCO ウィザードのパス

```
/usr/local/cliqr/bin/cco_config_wizard.sh
```

サーバのプロパティを設定します。

今後の参照のためにこれを書き留めてください。
後で使用できるように、「*インストール方法*」>「*メモ*」セクションを印刷したものにフィールドの詳細を書き留めてください。

ウィザード メニュー	フィールド	注記（Notes）
エージェント バンドル パラメータ（Agent Bundle Parameters）	Linux バンドル URL（Linux Bundle URL）	管理エージェント バンドルの Linux URL – デフォルトを使用するか、cdn.cliqr.com をカスタム バンドル ストア IP または DNS に置き換えます。
	Windows バンドル URL（Windows Bundle URL）	管理エージェント バンドルの Windows URL – デフォルトを使用するか、cdn.cliqr.com をカスタム バンドル ストア IP または DNS に置き換えます。
	ブートストラップ js URL（Bootstrap js URL）	動的ブートストラップ情報では必須 – デフォルトを使用するか、cdn.cliqr.com をローカル リポジトリ IP または DNS に置き換えます。 このフィールドは、次の 3 つのパッケージ ストア URL を示します。 • CloudCenter インストーラ パッケージ：http://${s3Bucket}/${imageBootstrapperPath}/bundle/cliqrInstaller.zip • コア インストーラ パッケージ：http://${s3Bucket}/${imageBootstrapperPath}/bundle/corePkg.tar.gz • JSON パッケージ：http://${s3Bucket}/${imageBootstrapperPath}/bundle/simplejson.tar.gz
	ブートストラップ py URL（Bootstrap py URL）	Linux ファイルに呼び出される動的ブートストラップ情報では必須 – デフォルトを使用するか、cdn.cliqr.com をカスタム バンドル ストア IP または DNS に置き換えます。

	ブートストラップ Linux URL（Bootstrap Linux URL）	Linux ファイルの動的ブートストラップ情報では必須 – デフォルトを使用するか、cdn.cliqr.com をカスタム バンドル ストア IP または DNS に置き換えます。
	ブートストラップ win URL（Bootstrap win URL）	Windows ファイルの動的ブートストラップ情報では必須 – デフォルトを使用するか、cdn.cliqr.com をカスタム バンドル ストア IP または DNS に置き換えます。
	Linux アップグレード URL（Linux Upgrade URL）	管理エージェントアップグレード スクリプトの Linux URL - デフォルトを使用するか、cdn.cliqr.com をカスタム バンドル ストア IP または DNS に置き換えます。
	Windows アップグレード URL（Windows Upgrade URL）	管理エージェント アップグレード スクリプトの Windows URL – デフォルトを使用するか、cdn.cliqr.com をカスタム バンドル ストア IP または DNS に置き換えます。
	ノード メタデータ URL（Node Metadata URL）	管理エージェント VM のメタデータ（.jar ファイル）URL - デフォルトを使用するか、cdn.cliqr.com をカスタム バンドル ストア IP または DNS に置き換えます。
	カスタム リポジトリ URL（Custom Repo URL）	CloudCenter カスタム アーティファクト リポジトリ URL - デフォルトを使用するか、repo.cliqrtech.com をカスタム パッケージ ストア IP または DNS に置き換えます。
	サービス URL（Service URL）	設定済みサービスをポイントする URL – デフォルトを使用するか、cdn.cliqr.com をカスタム バンドル ストア IP または DNS に置き換えます。
	アクション URL（Action URL）	この URL は、サービス ライフサイクル アクションまたは VM アクションを実行するときにスクリプトをダウンロードできる VM の場所をポイントする必要があります（HTTP URL にはこの VM からアクセス可能である必要があります）。
	AgentLite Linux URL	Linux ベースの agent-lite-linux-bundle.tar.gz が存在する場所。この URL は、Linux VM で AgentLite をインストールする（「VM Management」>「*Install Agent Manually*」を参照）ために必要です。
	AgentLite Windows URL	Windows ベースの agent-lite-windows-bundle.zip が存在する場所。この URL は、Windows VM で AgentLite をインストールする（「VM Management」>「*Install Agent Manually*」を参照）ために必要です。
	外部サービス URL（External Service URL）	外部サービス バンドルへのパス/URL – デフォルトを使用するか、cdn.cliqr.com をカスタム バンドル ストア IP または DNS に置き換えます。
AMQP_Server	AMQP Server IP	AMQP_IP または AMQP_LB_IP
	AMQPポート（AMQP Port）	5671
ネットワーク（Network）	ホストネーム（Hostname）	CCO 環境のネットワークの詳細を設定します。これは、VM のプライベート IP を設定するオプションの手順です。VM の IP またはホスト名が事前に設定されていない場合、または既存の IP またはホスト名を上書きする必要がある場合は、一般に次の情報を設定できます。
Guacamole	接続ブローカ ホスト（Connection Broker Hos）	AMQP_IP または AMQP_LB_IP
	接続ブローカ ポート（Connection Broker Port）	7788
	Connection Broker Port2	7789
Docker	Docker Registry URL	カスタム Docker レジストリが使用されたときだけ設定します。
	Docker CACert URL	Docker レジストリでカスタム CA 証明書を使用して SSL を使用しているときだけ設定します。 詳細については、「Certificate Authentication」>「*Dedicated Components*」を参照してください。
ELK_Info	ELK ホスト（ELK Host）	ELK/モニタ ホストの IP アドレスを指定します。
	Elasticsearch ポート（Elasticsearch Port）	8881 がデフォルトで表示されます。

	Logstash ポート（Logstash Port）	4560 がデフォルトで表示されます。
	ホスト識別子（Host Identifier）	サーバの一意の ID：固有識別子の前に必ず、CCO_ を追加してください（例：CCO_Openstack_regionOne または CCO_Amazon_east）。
	ホスト識別子のリスト（Host Identifier List）	このフィールドは HA モードを使用する環境にのみ適用：HA セットアップのすべての ELK/モニタ ホストに対してカンマ区切りの一意のホスト識別子のリストを提供します（例：CCO1,CCO2,myCCO）。 HA モードで動作する環境では、それぞれの server.properties ファイルに CCO_1,CCO_2,CCO_3 として固有 ID が設定されている 3 つの CCO インスタンスがある場合、このプロパティは各 CCO インスタンスで **CCO_1,CCO_2,CCO_3** と示す必要があります。各 CCO は HA モードの他の CCO の固有 ID を認識する必要があります。
External_Script_Executor	Docker サーバ IP（Docker Server IP）	デフォルト IP は 127.0.0.1 です。 該当する場合は、専用の Docker サーバの IP アドレスを入力します。
	Docker サーバ ポート（Docker Server Port）	デフォルトは 2376 です
Config_Certs	証明書 Zip パス（Certs Zip Path）	certs.zip ファイルのパスを指定します。デフォルト パスは /tmp/certs.zip です。

1. 変更を確認し、CCO 設定ウィザードを終了します。
2. Tomcat Service を再起動して変更を適用するには、[はい（Yes）] を選択します。

CCO インスタンスは正常に設定されました。これで、次のステップに進むことができます。

- CCO HA を設定している場合：「*CCO_LB*」を参照して HA 設定を完了します。
- 専用の Docker コンポーネントをインストールしている場合：「*専用の Docker レジストリ インストール（オプション）*」を参照してください。
- 専用の Docker コンポーネントをインストールしていない場合：「管理者アカウントの設定」を参照し、CloudCenter の設定およびセットアップを続行してください。

CCO HA

アプライアンスを使用する CCO HA のインストール

- CCO SSH キーの交換
- CCO_PRIMARY - CCO のプロパティの設定
- CCO ウィザードのプロパティの設定
- CCO_LB

CCO SSH キーの交換

CCO_PRIMARY、CCO_SECONDARY、CCO_TERTIARY インスタンス間で SSH キーを交換するには、次の手順に従います。

1. CCO_PRIMARY インスタンスで、次のコマンドを実行し、新しい SSH キーを生成します。

```
sudo -i
ssh-keygen -t rsa
cd ~/.ssh
cat id_rsa.pub >> authorized_keys
```

2. CCO_PRIMARY から CCO_SECONDARY および CCO_TERTIARY の同じ場所に id_rsa ファイル（~/.ssh/id_rsa と ~/.ssh/id_rsa.pub）をコピーします。CCO_SECONDARY および CCO_TERTIARY で、.ssh ディレクトリがない場合は、ファイルをコピーする前に、次のコマンドを使用して作成します。

```
sudo -i
mkdir -p ~/.ssh
chmod 700 ~/.ssh
```

3. CCO_SECONDARY および CCO_TERTIARY で、次のコマンドを実行し、新しい SSH キーを追加します。

```
sudo -i
chmod 400 ~/.ssh/id_rsa*
cat id_rsa.pub >> authorized_keys
```

4. 各 VM 上で次のコマンドを実行して、CCO_PRIMARY、CCO_SECONDARY、および CCO_TERTIARY 間の相互 SSH アクセスを確認します。

```
sudo -i
ssh root@<CCO_PRIMARY/CCO_SECONDARY/CCO_TERTIARY>
```

3 つすべての CCO インスタンスに SSH が設定されました。

CCO_PRIMARY - CCO のプロパティの設定

CCO_PRIM ARY ウィザード***のみ***で次の詳細を提供することにより、3 つすべての CCO サーバの情報を設定できます。

3 つすべての CCO が相互に通信するようにするには、**CCO_PRIMARY** ウィザードで次の HA 固有の情報を設定する必要があります。

ウィザード メニュー	フィールド	注記（Notes）
Configure_HA CCO HA 情報（CCO HA Info）：プライマリ CCO サーバで次の詳細を指定します。	プライマリ ノード IP（Primary Node IP）	プライマリ CCO インスタンスの IP アドレスを入力します。
	セカンダリ ノード IP（Secondary Node IP）	セカンダリ CCO インスタンスの IP アドレスを入力します。
	ターシャリ ノード IP（Tertiary Node IP）	ターシャリ CCO インスタンスの IP アドレスを入力します

上記の HA 固有の情報に加え、**CCO_PRIMARY** ウィザードの汎用情報も設定する必要があります。

CCO ウィザードのプロパティの設定

このコンポーネントは、クラウド リージョンごと（パブリック クラウド、プライベート クラウド、またはデータセンター）に必要です。

1. CCO ウィザードを起動するには、次のプロセスに従います。
   a. CCO インスタンスに *centos* ユーザとして SSH 接続します。
   b. 次のコマンドを実行します。

```
sudo -i
```

- CCO ウィザードを起動します。

CCO ウィザードのパス
/usr/local/cliqr/bin/cco_config_wizard.sh

サーバのプロパティを設定します。

今後の参照のためにこれを書き留めてください。
後で使用できるように、「*インストール方法*」>「*メモ*」セクションを印刷したものにフィールドの詳細を書き留めてください。

ウィザード メニュー	フィールド	注記（Notes）
エージェント バンドル パラメータ（Agent Bundle Parameters）	Linux バンドル URL（Linux Bundle URL）	管理エージェント バンドルの Linux URL – デフォルトを使用するか、cdn.cliqr.com をカスタム バンドル ストア IP または DNS に置き換えます。
	Windows バンドル URL（Windows Bundle URL）	管理エージェント バンドルの Windows URL – デフォルトを使用するか、cdn.cliqr.com をカスタム バンドル ストア IP または DNS に置き換えます。
	ブートストラップ js URL（Bootstrap js URL）	動的ブートストラップ情報では必須 – デフォルトを使用するか、cdn.cliqr.com をローカル リポジトリ IP または DNS に置き換えます。 このフィールドは、次の 3 つのパッケージ ストア URL を示します。 • CloudCenter インストーラ パッケージ：http://${s3Bucket}/${imageBootstrapperPath}/bundle/cliqrInstaller.zip • コア インストーラ パッケージ：http://${s3Bucket}/${imageBootstrapperPath}/bundle/corePkg.tar.gz • JSON パッケージ：http://${s3Bucket}/${imageBootstrapperPath}/bundle/simplejson.tar.gz
	ブートストラップ py URL（Bootstrap py URL）	Linux ファイルに呼び出される動的ブートストラップ情報では必須 – デフォルトを使用するか、cdn.cliqr.com をカスタム バンドル ストア IP または DNS に置き換えます。
	ブートストラップ Linux URL（Bootstrap Linux URL）	Linux ファイルの動的ブートストラップ情報では必須 – デフォルトを使用するか、cdn.cliqr.com をカスタム バンドル ストア IP または DNS に置き換えます。
	ブートストラップ win URL（Bootstrap win URL）	Windows ファイルの動的ブートストラップ情報では必須 – デフォルトを使用するか、cdn.cliqr.com をカスタム バンドル ストア IP または DNS に置き換えます。
	Linux アップグレード URL（Linux Upgrade URL）	管理エージェントアップグレード スクリプトの Linux URL - デフォルトを使用するか、cdn.cliqr.com をカスタム バンドル ストア IP または DNS に置き換えます。
	Windows アップグレード URL（Windows Upgrade URL）	管理エージェント アップグレード スクリプトの Windows URL – デフォルトを使用するか、cdn.cliqr.com をカスタム バンドル ストア IP または DNS に置き換えます。
	ノード メタデータ URL（Node Metadata URL）	管理エージェント VM のメタデータ（.jar ファイル）URL - デフォルトを使用するか、cdn.cliqr.com をカスタム バンドル ストア IP または DNS に置き換えます。
	カスタム リポジトリ URL（Custom Repo URL）	CloudCenter カスタム アーティファクト リポジトリ URL - デフォルトを使用するか、repo.cliqrtech.com をカスタム パッケージ ストア IP または DNS に置き換えます。
	サービス URL（Service URL）	設定済みサービスをポイントする URL – デフォルトを使用するか、cdn.cliqr.com をカスタム バンドル ストア IP または DNS に置き換えます。
	アクション URL（Action URL）	この URL は、サービス ライフサイクル アクションまたは VM アクションを実行するときにスクリプトをダウンロードできる VM の場所をポイントする必要があります（HTTP URL にはこの VM からアクセス可能である必要があります）。
	AgentLite Linux URL	Linux ベースの agent-lite-linux-bundle.tar.gz が存在する場所。この URL は、Linux VM で AgentLite をインストールする（「VM Management」>「*Install Agent Manually*」を参照）ために必要です。
	AgentLite Windows URL	Windows ベースの agent-lite-windows-bundle.zip が存在する場所。この URL は、Windows VM で AgentLite をインストールする（「VM Management」>「*Install Agent Manually*」を参照）ために必要です。
	外部サービス URL（External Service URL）	外部サービス バンドルへのパス/URL – デフォルトを使用するか、cdn.cliqr.com をカスタム バンドル ストア IP または DNS に置き換えます。
AMQP_Server	AMQP Server IP	AMQP_IP または AMQP_LB_IP
	AMQPポート（AMQP Port）	5671
ネットワーク（Network）	ホストネーム（Hostname）	CCO 環境のネットワークの詳細を設定します。これは、VM のプライベート IP を設定するオプションの手順です。VM の IP またはホスト名が事前に設定されていない場合、または既存の IP またはホスト名を上書きする必要がある場合は、一般に次の情報を設定できます。

Guacamole	接続ブローカ ホスト（Connection Broker Hos）	AMQP_IP または AMQP_LB_IP
	接続ブローカ ポート（Connection Broker Port）	7788
	Connection Broker Port2	7789
Docker	Docker Registry URL	カスタム Docker レジストリが使用されたときだけ設定します。
	Docker CACert URL	Docker レジストリでカスタム CA 証明書を使用して SSL を使用しているときだけ設定します。 詳細については、「Certificate Authentication」>「*Dedicated Components*」を参照してください。
ELK_Info	ELK ホスト（ELK Host）	ELK/モニタ ホストの IP アドレスを指定します。
	Elasticsearch ポート（Elasticsearch Port）	8881 がデフォルトで表示されます。
	Logstash ポート（Logstash Port）	4560 がデフォルトで表示されます。
	ホスト識別子（Host Identifier）	サーバの一意の ID：固有識別子の前に必ず、CCO_ を追加してください（例：CCO_Openstack_regionOne または CCO_Amazon_east）。
	ホスト識別子のリスト（Host Identifier List）	このフィールドは HA モードを使用する環境にのみ適用：HA セットアップのすべての ELK/モニタ ホストに対してカンマ区切りの一意のホスト識別子のリストを提供します（例：CCO1,CCO2,myCCO）。 HA モードで動作する環境では、それぞれの server.properties ファイルに CCO_1,CCO_2,CCO_3 として固有 ID が設定されている 3 つの CCO インスタンスがある場合、このプロパティは各 CCO インスタンスで **CCO_1,CCO_2,CCO_3** と示す必要があります。各 CCO は HA モードの他の CCO の固有 ID を認識する必要があります。
External_Script_Executor	Docker サーバ IP（Docker Server IP）	デフォルト IP は 127.0.0.1 です。 該当する場合は、専用の Docker サーバの IP アドレスを入力します。
	Docker サーバ ポート（Docker Server Port）	デフォルトは 2376 です
Config_Certs	証明書 Zip パス（Certs Zip Path）	certs.zip ファイルのパスを指定します。デフォルト パスは /tmp/certs.zip です。

1. 変更を確認し、CCO 設定ウィザードを終了します。
2. Tomcat Service を再起動して変更を適用するには、[はい（Yes）] を選択します。

CCO インスタンスは正常に設定されました。これで、次のステップに進むことができます。

- CCO HA を設定している場合：「*CCO_LB*」を参照して HA 設定を完了します。
- 専用の Docker コンポーネントをインストールしている場合：「*専用の Docker レジストリ インストール（オプション）*」を参照してください。
- 専用の Docker コンポーネントをインストールしていない場合：「管理者アカウントの設定」を参照し、CloudCenter の設定およびセットアップを続行してください。

CCO_LB

ロード バランシングは、HAProxy、NGiNX、Apache2、または AWS Elastic ロード バランサ（ELB）などのサービスをネイティブで使用できるクラウドで実行できます。ロード バランサ サービスを設定し、CCO ロード バランシングを確認するには、ポート 8443 でリスニングし、CCO_PRIMARY および CCO_SECONDARY サーバの両方のポート 8443 で要求を調整してください。

導入のためにオープンにする必要があるポートの完全なリストについては、「CCO ファイアウォール ルール」>「*CCO_LB ポート*」を参照してください。

> CloudCenter コンポーネントのロード バランサを設定する場合は、firewalld がデフォルトで有効になっていることに注意してください。CloudCenter コンポーネントがロード バランサと通信できるようにするには、明示的に無効にする必要があります。詳細については、「ファイアウォール ルールの概要」を参照してください。

次のロード バランシング設定が CCO VM の HAProxy と CentOS7.x VM で行われました。

1. CCO VM を起動するために使用するキー ペアを使用して VM インスタンスに SSH 接続します。
2. ルート ユーザとして HAProxy をインストールします。

```
yum install -y haproxy
```

3. 次のように、HAProxy の設定ファイルを変更します。

```
vi /etc/haproxy/haproxy.cfg

# listen on 8443 with SSL certs and loadbalance
frontend httpsalt-in
    mode tcp
    log global
    bind *:8443
    default_backend ccos

backend ccos
    mode tcp
    balance roundrobin
    option ssl-hello-chk
    server  cco1 <CCO_PRIMARY_IP>:8443
    server  cco2 <CCO_SECONDARY_IP>:8443
    server  cco3 <CCO_TERTIARY_IP>:8443
```

4. HAProxy サービスを開始し、そのステータスがアクティブであることを確認します

```
systemctl start haproxy
systemctl status haproxy
```

管理エージェント（ワーカー）のインストール

- 仮想アプライアンスの方法
- ブートストラップ メカニズムの方法
- HTTPS の依存関係

ワーカー アプライアンスには、CloudCenter に導入されたすべてのアプリケーション VM にプッシュされる Java ベース管理エージェントの仮想アプライアンスが含まれます。このファイルは OS 固有であり、Linux サーバでのみ利用可能です。

> ライセンスの問題のため、仮想アプライアンスはカスタムの Windows イメージでは利用できません。
>
> カスタムの Windows イメージをインストールするには、インストーラの方法を使用することをお勧めします。インストーラの方法を使用するには、CloudCenter サポート チームにお問い合わせください。

必要な VM にファイルをダウンロードしたら、CloudCenter プラットフォームはエージェントが不足していないかどうかを検出し、プロビジョニング時に自動的にエージェントを VM にプッシュします。

ワーカー イメージをアップロードする 2 つのオプションがあるため、必要なときに起動することができます。

- worker1 仮想アプライアンス
- ブートストラップ メカニズム

> このコンポーネントは、動的ブートストラップをサポートしないクラウドでは必須です。「Base OS Images」セクションで示されている表を参照して、ブートストラップ メカニズムを使用するかどうかを特定します。

仮想アプライアンスの方法

1. 「Virtual Appliances 」を参照し、必要なイメージをダウンロードするか共有するかを特定します。
2. 「仮想アプライアンスのプロセス」の説明に従って、イメージを Linux アプリケーション仮想アプライアンスにアップロードします。
3. 「イメージ マッピング」の説明に従って、アップロードされたイメージ ID をワーカー インスタンスで提供します。

ブートストラップ メカニズムの方法

詳細については、「Dynamic Bootstrapping」と「Dynamic Bootstrapping Support」を参照してください。

HTTPS の依存関係

バンドル ストアの設定手順では、デフォルトで HTTP プロトコルを使用します。HTTPS を使用してセキュアな接続を確保する場合は、次の要件に従います。

- CCO サーバ上の Docker イメージは、アップグレードが必要な場合があります。詳細については、「Docker Image Upgrade」を参照してください。
- ワーカー イメージで証明書をインストール済みにします。
- クラウドの依存関係を確認します。たとえば、クラウドが Linux VM を動的ブートストラップするために Python スクリプトを実行している場合は、Linux ワーカー イメージが Python バージョン 2.7.9 以降を使用することに注意してください。

> ワーカー イメージは、動的ブートストラップ用に Python スクリプトを使用するには、Python バージョン 2.7.9 以降を必要とします。
>
> 追加のソフトウェアをインストールする必要がある場合、管理者は **cliqruser** ロールに明示的な権限を割り当てる必要があります。
>
> セキュリティ強化の一環として、CloudCenter のすべてのコンポーネントの umask 設定は 077 に設定されています。このため、追加のソフトウェアをインストールするには、unmask ルールを 022 に設定する必要があります。

- また、Python スクリプトでは、HTTPS 証明書の検証をサポートするため、openssl-devel ライブラリをインストールする必要があります。

CloudCenter の設定

- 管理者アカウントの設定
- クラウドの設定
- CCM への CCO の登録
- イメージ マッピング
- インスタンス タイプの管理
- クラウド ストレージの設定
- イメージ ID の設定

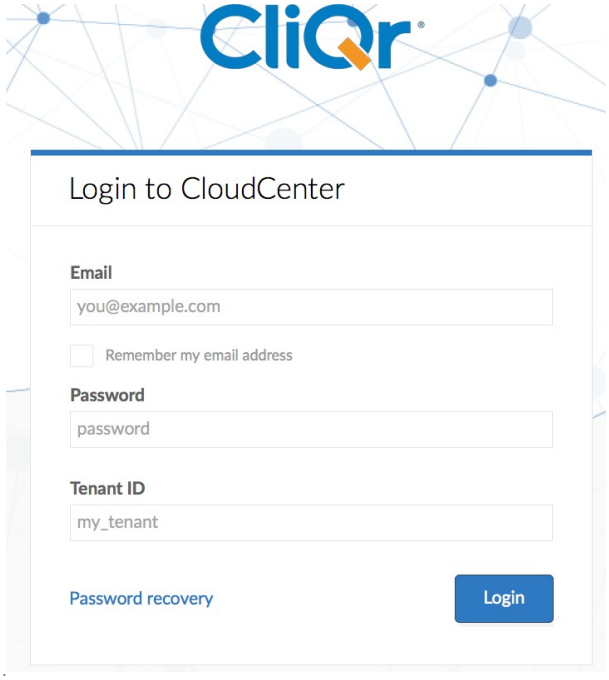
管理者アカウントの設定

- 管理者アカウントの設定
- 使用プランの作成
- 契約の作成
- 管理者への契約とプランの割り当て

管理者アカウントの設定

CCM VM を設定したら、ルート テナントの CloudCenter プラットフォーム管理者（admin）のアカウントを設定する必要があります。

1. ブラウザを開き、CCM VM の IP アドレス（たとえば、https://<CCM_IP>）を使用して CCM VM に接続します。



2. デフォルトの管理者クレデンシャルを使用してログインします。
   ユーザ名：admin@cliqrtech.com
   パスワード：cliqr

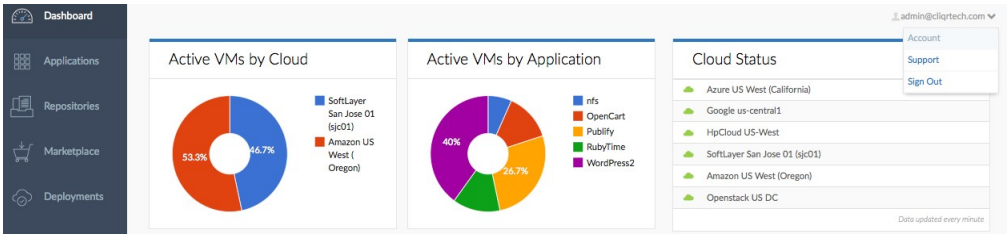
   [テナント ID（Tenant ID）] フィールドはオプションであり、この時点では空白のままにできます。

3. デフォルトのクレデンシャルを変更します。

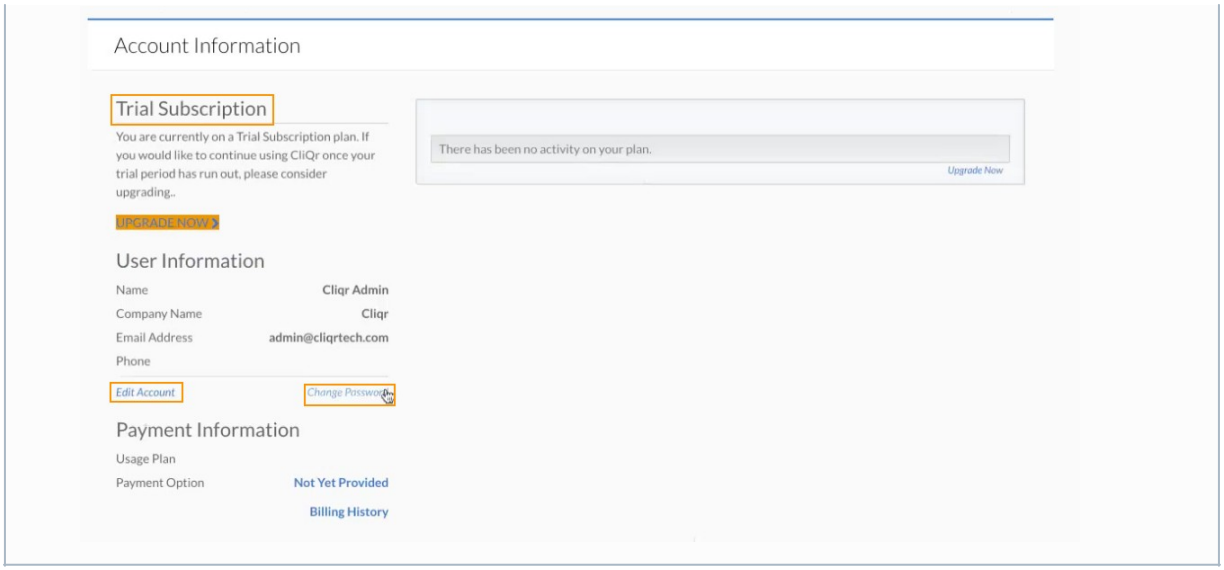
   最初のログイン後は、管理者アカウントの電子メールアドレスとパスワードを必ず変更してください。

   デフォルトのクレデンシャルを変更するには、次の手順に従います。

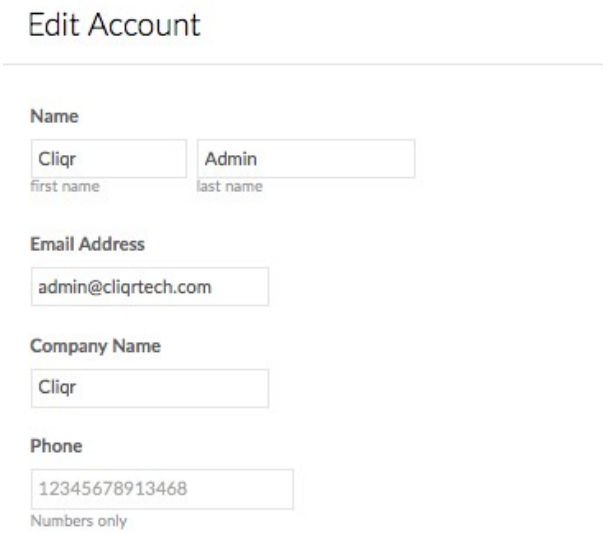
   a. CCM UI の右上隅に記された管理者の電子メールアドレスをクリックし、[アカウント（Account）] を選択して、このアカウントの [アカウント情報（Account Information）] ページにアクセスします。



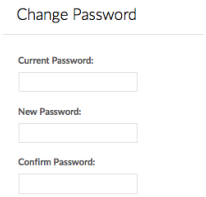
コメント
プランをまだ設定していない場合、現在のプランとして [試用版サブスクリプション（Trial Subscription）] が表示されます。



b. [アカウントの編集（Edit Account）] をクリックしてアカウント名、電子メールアドレス、会社名、電話番号を編集し、[保存（Save）] をクリックします。



c. パスワードを変更するには、[パスワードの変更（Change Password）] をクリックします。新しいパスワードを保存します。

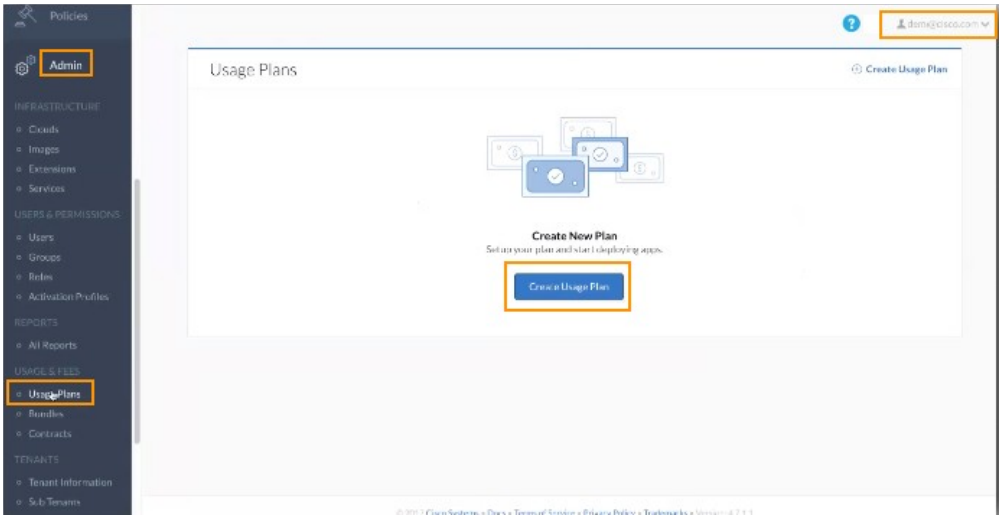


d. CCM UI（右上隅のドロップダウン）からサインアウトし、新しいクレデンシャルを使用してログインします。新しい電子メールアドレスは、CCM UI の右上隅に表示されます。

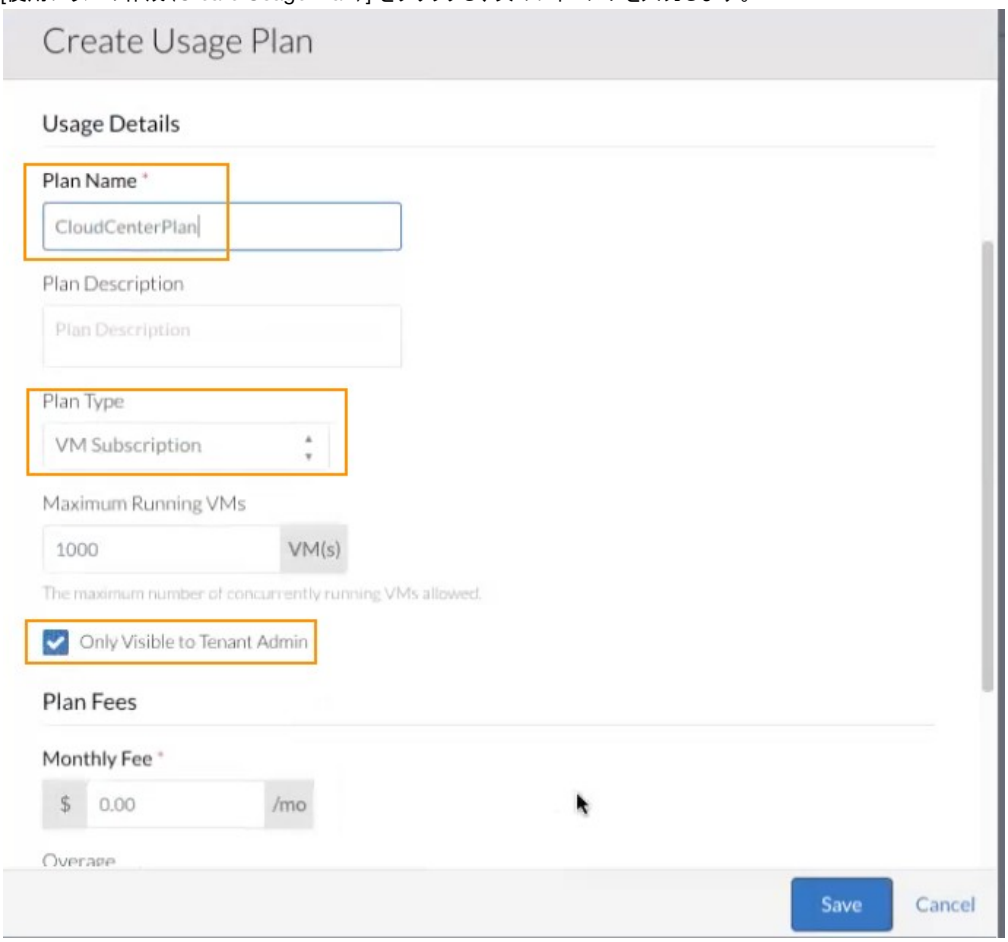
使用プランの作成

CloudCenter インスタンスの使用プランの選択 - 選択するプランにより、*すべてのテナントとユーザにおける* CloudCenter の使用が制限されます。詳細については、「Usage Plans and Fees」を参照してください。

1. CCM UI のメインメニューで、[管理（Admin）] > [使用プラン（Usage Plan）] をクリックします。



2. [使用プランの作成（Create Usage Plan）] をクリックし、次のフィールドを入力します。



a. [プラン名（Plan Name）] を指定します。
b. 使用要件に基づいて、[プランのタイプ（Plan Type）] フィールドでプランを選択します。
たとえば、[VM サブスクリプション（VM Subscription）] プランでは、毎月指定された VM を実行することができます。
c. [テナント管理者にのみ表示（Only Visible to Tenant Admin）] チェックボックスをオンにして、プランをテナント管理者にのみ表示するようにします。

> この設定は、ルート プラットフォーム管理者専用です。この管理者は、後でユーザ固有のプランを設定できます

d. オプション：[プランの各料金（Plan Fees）] セクションはこの時点では省略可能です。制限を設定し、超過料金を割り当てるため、後でこの情報を設定します。詳細については、「Usage Plans and Fees」を参照してください。
e. [保存（Save）] をクリックします。[使用プラン（Usage Plan）] ページに、この新しいプランが正常に追加されたことが表示されます。

契約の作成

CloudCenter インスタンスのコントラクトを選択します。選択したプランにより、CloudCenter の使用が指定された期間に制限されます。

1. 管理者用の契約を作成するには、次の手順を実行します。
   a. CCM UI のメインメニューで、[管理(Admin)] > [使用プラン(Usage Plan)] > [コントラクトの作成(Create Contract)] をクリックして新しい契約の作成を開きます。

   > 現在の CloudCenter ライセンス契約書は、信頼に基づいたものです。

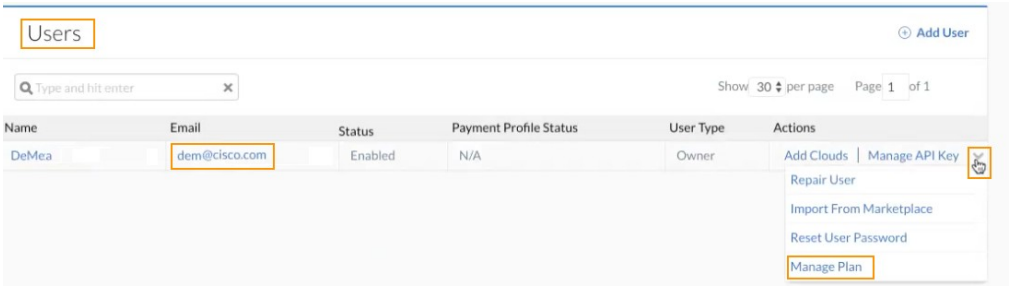
   b. 契約に該当する情報を入力し、[送信(Submit)] をクリックします。

   > [管理者にのみ表示(Only Visible to Admin)] チェックボックスをオン(設定をルート プラットフォーム管理者に対してのみ適用)にしてプランを管理者だけに表示するようにします。

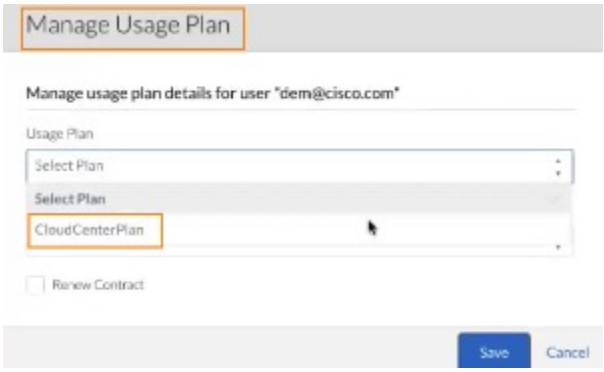
管理者への契約とプランの割り当て

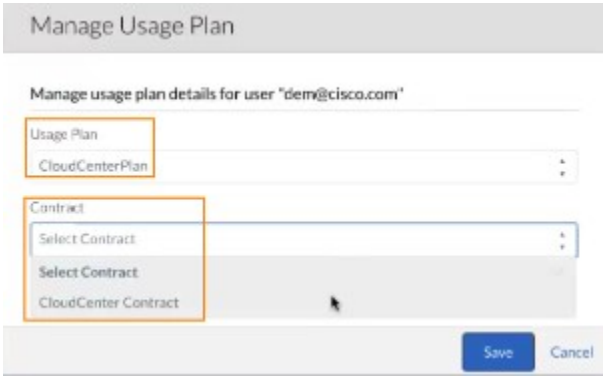
契約とプランをプラットフォーム管理者に割り当てる必要があります。

1. CCM UI のメインメニューで [管理(Admin)] > [ユーザ(Users)] をクリックし、ユーザ管理ページにアクセスします。



2. 電子メールを検索し、[アクション(Actions)] ドロップダウン リストから [プランの管理(Manage Plans)] を選択します。
3. 作成したプランと契約を検索し、それらをこのプラットフォーム管理者に割り当てます。





4. [保存(Save)] をクリックします。

> CloudCenter のプラットフォームを効果的に使用し続けるために、必ず、この時点で契約条項に同意してください。

CloudCenter の導入では各 CCO のクラウドの設定を行うことができます。

クラウドおよびクラウド アカウントの設定

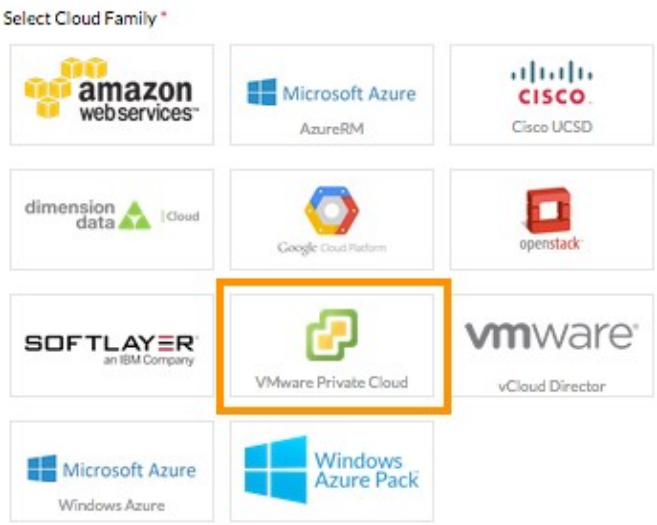
このセクションでは、サポートされている各クラウドを設定するための手順の例を示します。各手順をガイドラインとして、任意のクラウドを設定してください。

- VMware クラウドの設定

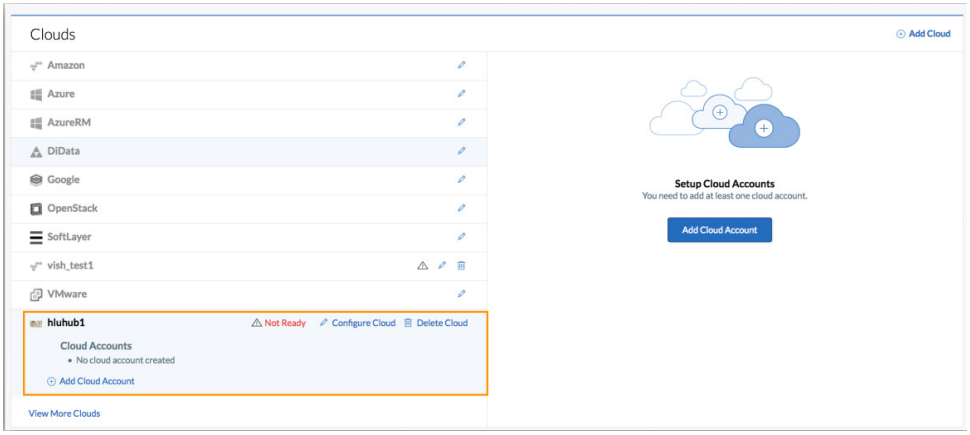
VMware クラウドの設定

VMware クラウドで論理マッピングを設定するには、次のプロセスに従います。

1. CCM UI にアクセスし、CCM UI のメインメニューで [管理(Admin)] > [クラウド(Clouds)] > [クラウドの追加(Add Cloud)] を選択します。



2. [VMware プライベート クラウド（VMware Private Cloud）] オプションを選択し、このクラウドの名前と説明を入力して、[保存（Save）] をクリックします。
3. 新たに追加されたクラウドを見つけて [クラウド アカウントの追加（Add Cloud Account）] ボタンをクリックし、このクラウド ファミリにアカウントを追加します。



4. [クラウド アカウントの追加（Add Cloud Account）] をクリックして、このクラウド ファミリにアカウントを追加します。[クラウド アカウントの追加（Add Cloud Account）] ポップアップが表示されます。
   a. 新しいクラウドに**名前**を割り当てます。
   b. [クラウド コストの追跡（Track Cloud Costs）] チェックボックスをオンにして、クラウド コストを追跡します。
   c. vCenter アカウントの詳細を入力します。

クラウド アカウントの詳細	説明
vCenter アドレス（vCenter Address）	このアカウントに設定する IP アドレス。
vCenter ユーザ名/パスワード（vCenter User Name/Password）	このクラウド アカウントにアクセスするためのクレデンシャル。必要なアクセス許可については、次の表を参照してください。

vCenter ユーザに完全な管理者権限がない場合は、（CloudCenter を使用する）各ユーザに少なくとも次のアクセス許可があることを確認してください。

vCenter オブジェクト	必要なアクセス許可	理由（Reason）
ネットワーク（Network）	ネットワークの割り当て	テンプレート/スナップショットのデフォルトのネットワークを変更する必要がある場合
データストア	領域の割り当て	永続的なディスク操作のため
	データストアの参照	
	低レベルのファイル操作	
	ファイルの削除	

フォルダ	フォルダの作成	ユーザのフォルダの作成のため
リソース	推奨事項の適用	データストア クラスタのサポートのため
	リソース プールへの VM の割り当て	リソース プールの選択のため
タスク	タスクの作成	VM の操作のため
	タスクの更新	
仮想マシン	すべてのアクセス許可	

d. [保存(Save)] をクリックし、新しく追加したクラウドが [クラウド設定(Cloud Configurations)] ページに表示されていることを確認します。

5. [リージョン(Region)] タブをクリックし、クラウド リージョンを追加します。
   a. [クラウド リージョンの追加(Add Cloud Region)] をクリックします。
   b. このクラウドに必要なリージョンを選択します。
   c. このクラウド リージョンの [リージョン名(Region Name)] およびオプションの [表示名(Display Name)] を追加します。
   d. [保存(Save)] をクリックします。

> インスタンス タイプ、ストレージ タイプ、およびイメージ マップのセクションは、リージョンを追加するとすぐに自動的に設定されます。

6. (任意)[クラウド設定の編集(Edit Cloud Settings)] をクリックし、[インスタンスの命名方法(Instance Naming Strategy)]、[インスタンス IPAM の使用(Instance IPAM Strategy)]、または [ノード名設定(Node Name Config)] フィールドを更新します。「VM Name Config」セクションでは、これらの値の設定の詳細を説明しています。

> **注意**
> **クラウド設定を編集**する場合、変更を CCO に保存し、これらの変更がファイアウォールの設定内の CCO にも反映されるようにする必要があります。
>
> CCO がすでに設定されている場合は、これらのクラウド設定を有効にするために CCO を再登録する必要があります。

7. クラウド設定を完了するには、CCO を CCM に登録する必要があります。
   CCM への CCO の登録

CCM への CCO の登録

- クラウド リージョンの微妙な違い
- 非 HA モード
- HA モード

クラウド リージョンの微妙な違い

CCM に CCO を登録すると、CCO は登録されたクラウド リージョンにのみ動作します。

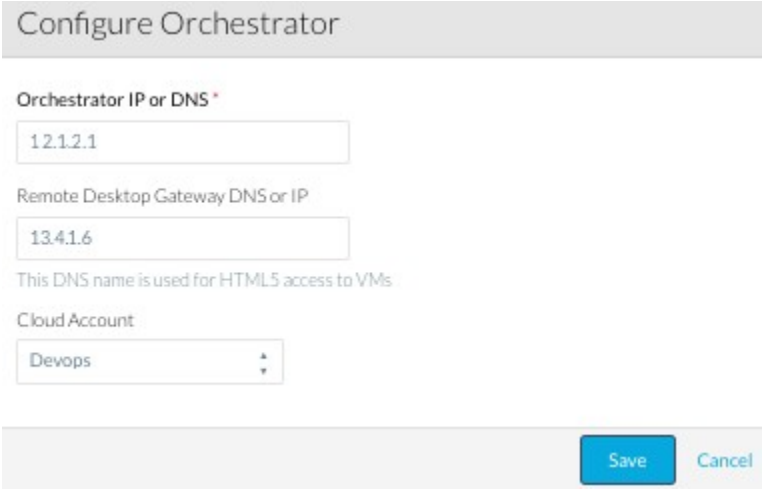
> **CloudCenter**
> CCM に CCO を登録すると、CloudCenter プラットフォームは、このクラウド リージョンがアクティブであると見なし、特定条件下でしか CloudCenter プラットフォームからこのクラウド リージョンを削除できなくなります。詳細については、「Cloud Region Configuration」>「*Delete Cloud Region*」を参照してください。

> 提供された例では AWS クラウドを参照していますが、スクリーン キャプチャはクラウドごとに異なることがある点に注意してください。

非 HA モード

CCM に CCO を登録するには、次の手順に従います。

a. [オーケストレータの設定(Configure Orchestrator)] ポップアップで、CCM からアクセス可能な CCO の IP アドレスを入力し、CCO をホストするために使用されるクラウド アカウントを選択します。



b. このページがまだ表示されていない場合は、必要なクラウドにおいて、[管理(Admin)] > [クラウド(Clouds)] > [リージョンの設定(Configure Regions)] を選択していることを確認します。
   i. [リージョン(Regions)] タブの [オーケストレータの設定(Configure Orchestrator)] をクリックします。
   ii. オーケストレータの IP または DNS(Orchestrator IP or DNS):CCO サーバの IP または DNS アドレスを指定します。
   iii. リモート デスクトップ ゲートウェイの DNS または IP(Remote Desktop Gateway DNS or IP):Guacamole サーバの IP アドレス(VM へのブラウザベースのアクセスを有効化)。Guacamole コンポーネントが AMQP サーバ内に存在している場合は、AMQP サーバの IP アドレスを指定します。
   iv. クラウド アカウント(Cloud Account):この CCO で使用するクラウド アカウントを選択します。

> **Amazon クラウドの微妙な違い**
> IAM ロールを設定している場合、この設定は重要です。必ずこのロールを含むクラウド アカウントを選択してください。

c. [保存(Save)] をクリックします。これで、CCM と CCO の相互信頼関係が確立されました。CloudCenter プラットフォームは現在、導入された CCO によりクラウド リージョンを管理しています。
d. 手順 2 と手順 3 を繰り返し、CCM とその他の CCO 間の相互信頼を確立します。

CCO VM を登録し、設定が完了しました。ここでは、2 つのオプションがあります。

- その他のクラウド リージョンを追加し、これらのクラウドごとに CCO を登録します。詳細については、「クラウド リージョンごと(必須)」を参照してください。
- イメージをマッピングします。詳細については、「イメージ マッピング」を参照してください。

> クラウド アカウントのイメージを起動するアクセス許可を付与する必要がある場合は、「Image Launch Permissions」を参照してください。

- アプリケーションのモデリング、展開、および管理を行います。詳細については、「Application Profile」を参照してください。

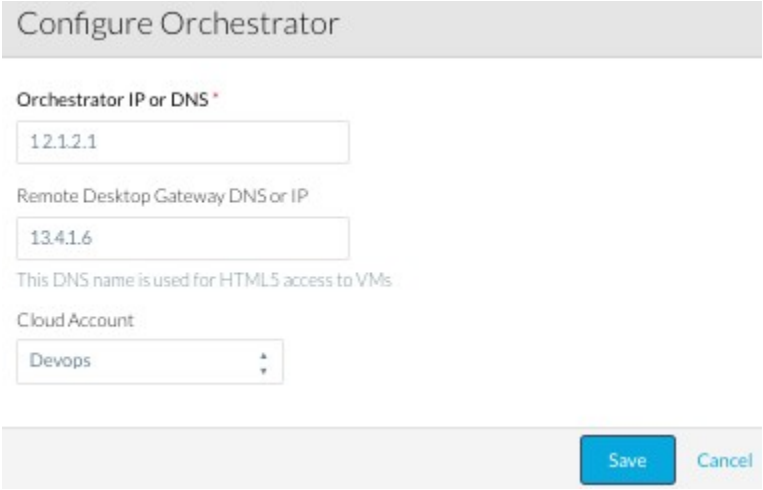
HA モード

CCM に CCO を登録するには、次の手順に従います。

a. プライマリ CCO で Tomcat Service が実行中であることを確認します。
b. セカンダリ CCO およびターシャリ CCO にログインし、両方のサーバで Tomcat Service を停止します。

```
/etc/init.d/tomcat stop
```

c. CCM UI にアクセスし、CCO LB の IP アドレスを使用して CCO を登録します。
   i. このページがまだ表示されていない場合は、必要なクラウドにおいて、[管理(Admin)] > [クラウド(Clouds)] > [リージョンの設定(Configure Regions)] を選択していることを確認します。
   ii. [リージョン(Regions)] タブの [オーケストレータの設定(Configure Orchestrator)] をクリックします。
   iii. CCM からアクセス可能な CCO の IP アドレスを入力し、CCO をホストするために使用されるクラウド アカウントを選択します。



1. オーケストレータの IP または DNS（Orchestrator IP or DNS）：CCO サーバの IP または DNS アドレスを指定します。
2. リモート デスクトップ ゲートウェイの DNS または IP（Remote Desktop Gateway DNS or IP）：Guacamole サーバの IP アドレス（VM へのブラウザベースのアクセスを有効化）。Guacamole コンポーネントが AMQP サーバ内に存在している場合は、AMQP サーバの IP アドレスを指定します。
3. クラウド アカウント（Cloud Account）：この CCO で使用するクラウド アカウントを選択します。必ずこのロールを含むクラウド アカウントを選択してください。
4. [保存（Save）] をクリックします。これで、CCM と CCO の相互信頼関係が確立されました。CloudCenter プラットフォームは現在、導入された CCO によりクラウド リージョンを管理しています。

d. 登録が成功したら、プライマリ CCO サーバにログインします。
e. プライマリ CCO の **/usr/local/osmosix/etc/** フォルダから、セカンダリ CCO およびターシャリ CCO の両サーバ上の**同じ場所**に **gateway_config.properties** ファイルをコピーします。
f. すべてのサーバのコピーしたファイルの所有権およびアクセス許可が次のようになっていることを確認します。
   - オーナー（Owner）= cliqruser
   - グループ権限（Group Permission）= 読み取りおよび書き込み
g. 必要な場合は、次のコマンドを実行して設定を変更します。

```
chown
cliqruser:cliqruser
/usr/local/osmosix/etc/gateway_config.properties
chmod 644 /usr/local/osmosix/etc/gateway_config.properties
```

h. 各サーバで次のコマンドを発行することによって、セカンダリ CCO とターシャリ CCO サーバで Tomcat を起動します。

```
/etc/init.d/tomcat start
```

i. HA モードのその他の CCO についてこの手順を繰り返し、CCM とその他の CCO 間の相互信頼を確立します。

CCO VM を登録し、設定が完了しました。ここでは、2 つのオプションがあります。

- その他のクラウド リージョンを追加し、これらのクラウドごとに CCO を登録します。詳細については、「クラウド リージョンごと（必須）」を参照してください。
- イメージをマッピングします。詳細については、「イメージ マッピング」を参照してください。

> クラウド アカウントのイメージを起動するアクセス許可を付与する必要がある場合は、「Image Launch Permissions」を参照してください。

- アプリケーションのモデリング、展開、および管理を行います。詳細については、「Application Profile」を参照してください。

戻る：クラウドの設定

- vCD クラウドの設定

vCD クラウドの設定

> 次のスクリーン キャプチャは、vCD が変更されると変わる可能性があることに注意してください。この項ではあくまでも参考として示しています。

前提条件

CloudCenter プラットフォームで vCD クラウドをマッピングする前に、次の要件を確認します。

- 有効な vCD クラウド アカウント。
- vCD クラウドと同じクラウド リージョンの CCO を起動します。
- 次の手順に従って、CCO サーバの vCD クラウド プロバイダーを有効にします。vCD クラウドを使用する場合、CCO サーバを設定する必要があります。

  CCO サーバの vCD クラウド プロバイダーを有効にするには、次の手順に従います。

  1. rest-api-schemas-8.10.0.jar および vcloud-java-sdk-8.10.0.jar ファイルを /usr/local/tomcat/webapps/ROOT/WEB-INF/lib ディレクトリにコピーします。

     > これらのコピーはシスコによって再頒布されないため、顧客はこれらのライブラリのコピーを使用する必要があります。8.10.0 バージョンが必要です

  2. vCD を設定します。
     a. 次のディレクトリに変更します。

     ```
     cd /usr/local/osmosix/bin directory
     ```

     b. vcdconfig を実行します。
     vcdconfig ファイルが存在しない場合は、software.cisco.com からファイルをダウンロードします。詳細については、「仮想アプライアンスの概要」を参照してください。
     c. 「クラウド タイプを入力してください（Please enter cloud type）」のプロンプトで、サイト アセスメントを実行したときに決定したクラウド名とリージョン名を指定し、Enter を押します。
     この情報の入力には次の形式を使用します。
     CloudName-RegionName。

     > 設定後は変更できないため、この情報は正確に入力してください。

     次に例を示します。
     i. vCD の場合：
     vCloud-CliQrWest; f
     ii. vCloud Air の場合：
     VCoudAir-CliQrWest
     d. 「Org VDC 共有ネットワークを入力してください（カンマ区切りの複数の文字列がサポートされます）（Please enter Org VDC shared network (comma separated multiple string supported)）」のプロンプトで、サイト アセスメントを実行したときに決定した vCloud OrgVdc 共有ネットワーク情報を入力し、Enter を押します。複数のエントリはスペースなしでカンマで区切ります。
     たとえば、orgnet1,orgnet2 とします。
     e. 「ストレージ プロファイルを入力してください（カンマ区切りの複数の文字列がサポートされます）（Please enter storage profile (comma separated multiple string supported)）」のプロンプトで、サイト アセスメントを実行したときに決定したストレージ プロファイル情報を入力し、Enter を押します。複数のエントリはスペースなしでカンマで区切ります。
     たとえば、tier1,tier2,tier3 とします。
     f. 「CCM アドレスを入力してください（Please enter CCM address）」のプロンプトで、CCM サーバの IP アドレスを入力します。
     g. 「CCO プライベート アドレスを入力してください（Please enter CCO private address）」のプロンプトで、ログイン先の CCO サーバのプライベート IP アドレスを入力し、Enter を押します。
     たとえば 10.0.2.1 と入力します。
     h. 「CCO パブリック アドレスを入力してください（Please enter CCO public address）」のプロンプトで、ログイン先の CCO サーバのパブリック IP アドレスを入力し、Enter を押します。
     設定ツールに入力した情報が表示され、必要なファイルが生成されます。
  3. Tomcat サーバを再起動して、CCO サーバが自動的に vcloud-java-sdk および rest-api-schemas jar ファイルを使用するようにします。

設定プロセス

vCD クラウドで論理マッピングを設定するには、次の手順に従います。

1. CCM UI にアクセスし、CCM UI のメインメニューで [管理（Admin）] > [クラウド（Clouds）] > [クラウドの追加（Add Cloud）] を選択します。

2. [VMware vCloud Director] オプションを選択し、このクラウドの名前と説明を入力して、[保存（Save）] をクリックします。
3. 新たに追加されたクラウドを見つけて [クラウド アカウントの追加（Add Cloud Account）] をクリックし、このクラウド ファミリにアカウントを追加します。[クラウド アカウントの追加（Add Cloud Account）] ポップアップが表示されます。
   a. 新しいクラウドに**名前**を割り当てます。
   b. [クラウド コストの追跡（Track Cloud Costs）] チェックボックスをオンにして、クラウド コストを追跡します。
   c. vCD ユーザの詳細を入力します。

クラウド アカウントの詳細	説明
vCloud 組織名（vCloud Organization Name）	このアカウントが属する vCloud 組織。
vCenter ユーザ名/パスワード（vCenter Username/Password）	サイト アセスメントを実行したときに決定した vCloud ユーザ名。
vCloud OrgVdc	サイト アセスメントを実行したときに決定した vCloud 組織 vDC。
vCloud OrgVdc 共有ネットワーク（vCloud OrgVdc Shared Network）	サイト アセスメントを実行したときに決定した vCloud 組織 vDC 共有ネットワーク。
vCloud 隔離ネットワーク（vCloud Isolated Network）	サイト アセスメントを実行したときに決定した vCloud 隔離ネットワーク。

vCenter ユーザに完全な管理者権限がない場合は、（CloudCenter を使用する）各ユーザに少なくとも次のアクセス許可があることを確認してください。

vCenter オブジェクト	必要なアクセス許可	理由（Reason）
ネットワーク（Network）	ネットワークの割り当て	テンプレート/スナップショットのデフォルトのネットワークを変更する必要がある場合
データストア	領域の割り当て	永続的なディスク操作のため
	データストアの参照	
	低レベルのファイル操作	
	ファイルの削除	
フォルダ	フォルダの作成	ユーザのフォルダの作成のため
リソース	推奨事項の適用	データストア クラスタのサポートのため
	リソース プールへの VM の割り当て	リソース プールの選択のため
タスク	タスクの作成	VM の操作のため
	タスクの更新	

仮想マシン	すべてのアクセス許可	

d. [保存(Save)] をクリックし、新しく追加したクラウドが [クラウド設定(Cloud Configurations)] ページに表示されていることを確認します。

4. [リージョン(Region)] タブをクリックし、クラウド リージョンを追加します。
   a. [リージョンの追加(Add Region)] をクリックします。
   b. このクラウドに必要なリージョンを選択します。
   c. このクラウド リージョンの [リージョン名(Region Name)] およびオプションの [表示名(Display Name)] を追加します。

   リージョン名は、vcdconfig ファイルで指定されたリージョン名と同じにする必要があります(上記の「*前提条件*」セクションを参照)。

   d. [保存(Save)] をクリックします。
5. (任意)[クラウド設定の編集(Edit Cloud Settings)] をクリックし、[クラウド設定の設定(Configure Cloud Settings)] ポップアップで値を更新します。

   注意
   クラウド設定を編集する場合、変更を CCO に保存し、これらの変更がファイアウォールの設定内の CCO にも反映されるようにする必要があります。

   CCO がすでに設定されている場合は、これらのクラウド設定を有効にするために CCO を再登録する必要があります。

フィールド	説明
vCloud エンドポイント URL(vCloud Endpoint URL)	基本の vCD URL。 例:https://vcd.example.com/ org サフィックスの URL は、CloudCenter プラットフォームで自動的に追加されま
ノード名設定(Node Name Config)	詳細については、「VM Name Config」を参照してください。

6. クラウド設定を完了するには、CCO を CCM に登録する必要があります。
   CCM への CCO の登録

CCM への CCO の登録

- クラウド リージョンの微妙な違い
- 非 HA モード
- HA モード

クラウド リージョンの微妙な違い

CCM に CCO を登録すると、CCO は登録されたクラウド リージョンにのみ動作します。

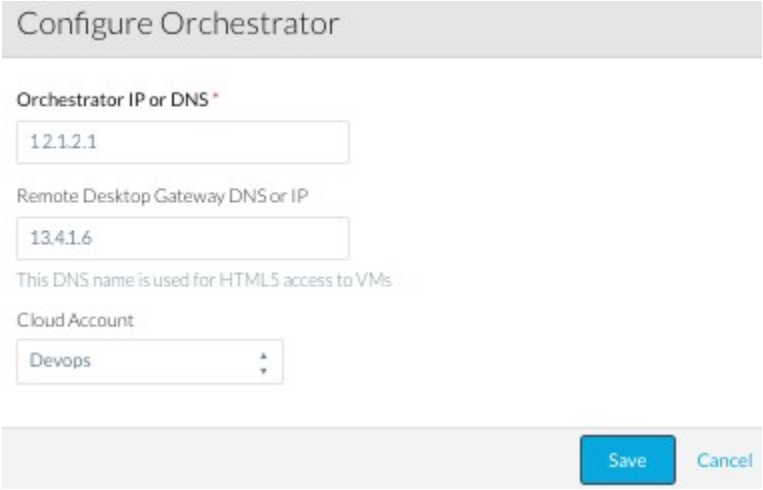
CloudCenter
CCM に CCO を登録すると、CloudCenter プラットフォームは、このクラウド リージョンがアクティブであると見なし、特定条件下でしか CloudCenter プラットフォームからこのクラウド リージョンを削除できなくなります。詳細については、「Cloud Region Configuration」>「*Delete Cloud Region*」を参照してください。

提供された例では AWS クラウドを参照していますが、スクリーン キャプチャはクラウドごとに異なることがある点に注意してください。

非 HA モード

CCM に CCO を登録するには、次の手順に従います。

a. [オーケストレータの設定(Configure Orchestrator)] ポップアップで、CCM からアクセス可能な CCO の IP アドレスを入力し、CCO をホストするために使用されるクラウド アカウントを選択します。



b. このページがまだ表示されていない場合は、必要なクラウドにおいて、[管理(Admin)] > [クラウド(Clouds)] > [リージョンの設定(Configure Regions)] を選択していることを確認します。
   i. [リージョン(Regions)] タブの [オーケストレータの設定(Configure Orchestrator)] をクリックします。
   ii. オーケストレータの IP または DNS(Orchestrator IP or DNS):CCO サーバの IP または DNS アドレスを指定します。
   iii. リモート デスクトップ ゲートウェイの DNS または IP(Remote Desktop Gateway DNS or IP):Guacamole サーバの IP アドレス(VM へのブラウザベースのアクセスを有効化)。Guacamole コンポーネントが AMQP サーバ内に存在している場合は、AMQP サーバの IP アドレスを指定します。
   iv. クラウド アカウント(Cloud Account):この CCO で使用するクラウド アカウントを選択します。

> **Amazon クラウドの微妙な違い**
> IAM ロールを設定している場合、この設定は重要です。必ずこのロールを含むクラウド アカウントを選択してください。

c. [保存(Save)] をクリックします。これで、CCM と CCO の相互信頼関係が確立されました。CloudCenter プラットフォームは現在、導入された CCO によりクラウド リージョンを管理しています。
d. 手順 2 と手順 3 を繰り返し、CCM とその他の CCO 間の相互信頼を確立します。

CCO VM を登録し、設定が完了しました。ここでは、2 つのオプションがあります。

- その他のクラウド リージョンを追加し、これらのクラウドごとに CCO を登録します。詳細については、「クラウド リージョンごと(必須)」を参照してください。
- イメージをマッピングします。詳細については、「イメージ マッピング」を参照してください。

> クラウド アカウントのイメージを起動するアクセス許可を付与する必要がある場合は、「Image Launch Permissions」を参照してください。

- アプリケーションのモデリング、展開、および管理を行います。詳細については、「Application Profile」を参照してください。

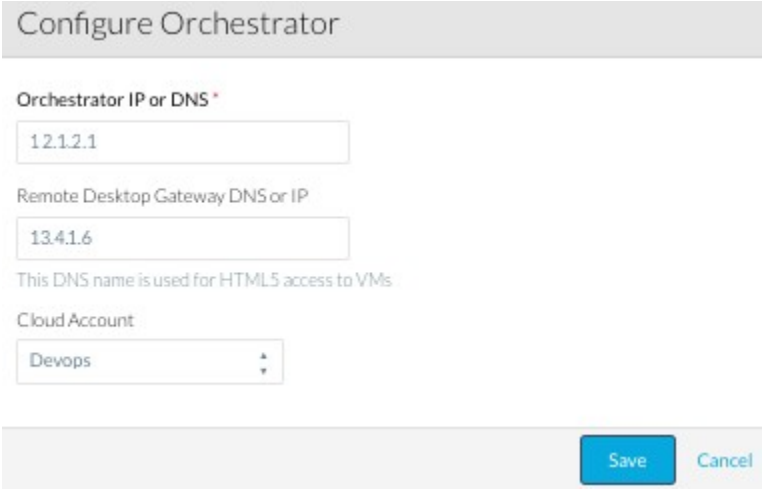
HA モード

CCM に CCO を登録するには、次の手順に従います。

a. プライマリ CCO で Tomcat Service が実行中であることを確認します。
b. セカンダリ CCO およびターシャリ CCO にログインし、両方のサーバで Tomcat Service を停止します。

```
/etc/init.d/tomcat stop
```

c. CCM UI にアクセスし、CCO LB の IP アドレスを使用して CCO を登録します。
   i. このページがまだ表示されていない場合は、必要なクラウドにおいて、[管理(Admin)] > [クラウド(Clouds)] > [リージョンの設定(Configure Regions)] を選択していることを確認します。
   ii. [リージョン(Regions)] タブの [オーケストレータの設定(Configure Orchestrator)] をクリックします。
   iii. CCM からアクセス可能な CCO の IP アドレスを入力し、CCO をホストするために使用されるクラウド アカウントを選択します。



1. オーケストレータの IP または DNS（Orchestrator IP or DNS）：CCO サーバの IP または DNS アドレスを指定します。
2. リモート デスクトップ ゲートウェイの DNS または IP（Remote Desktop Gateway DNS or IP）：Guacamole サーバの IP アドレス（VM へのブラウザベースのアクセスを有効化）。Guacamole コンポーネントが AMQP サーバ内に存在している場合は、AMQP サーバの IP アドレスを指定します。
3. クラウド アカウント（Cloud Account）：この CCO で使用するクラウド アカウントを選択します。必ずこのロールを含むクラウド アカウントを選択してください。
4. [保存（Save）] をクリックします。これで、CCM と CCO の相互信頼関係が確立されました。CloudCenter プラットフォームは現在、導入された CCO によりクラウド リージョンを管理しています。

d. 登録が成功したら、プライマリ CCO サーバにログインします。
e. プライマリ CCO の **/usr/local/osmosix/etc/** フォルダから、セカンダリ CCO およびターシャリ CCO の両サーバ上の**同じ場所**に **gateway_config.properties** ファイルをコピーします。
f. すべてのサーバのコピーしたファイルの所有権およびアクセス許可が次のようになっていることを確認します。
   - オーナー（Owner）= cliqruser
   - グループ権限（Group Permission）= 読み取りおよび書き込み
g. 必要な場合は、次のコマンドを実行して設定を変更します。

```
chown
cliqruser:cliqruser
/usr/local/osmosix/etc/gateway_config.properties
chmod 644 /usr/local/osmosix/etc/gateway_config.properties
```

h. 各サーバで次のコマンドを発行することによって、セカンダリ CCO とターシャリ CCO サーバで Tomcat を起動します。

```
/etc/init.d/tomcat start
```

i. HA モードのその他の CCO についてこの手順を繰り返し、CCM とその他の CCO 間の相互信頼を確立します。

CCO VM を登録し、設定が完了しました。ここでは、2 つのオプションがあります。

- その他のクラウド リージョンを追加し、これらのクラウドごとに CCO を登録します。詳細については、「クラウド リージョンごと（必須）」を参照してください。
- イメージをマッピングします。詳細については、「イメージ マッピング」を参照してください。

> クラウド アカウントのイメージを起動するアクセス許可を付与する必要がある場合は、「Image Launch Permissions」を参照してください。

- アプリケーションのモデリング、展開、および管理を行います。詳細については、「Application Profile」を参照してください。

戻る：クラウドの設定

- SoftLayer クラウドの設定

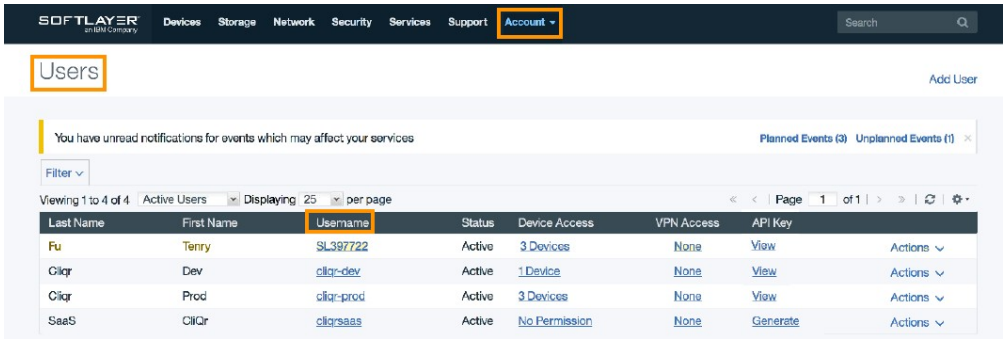
SoftLayer クラウドの設定

> 次のスクリーン キャプチャは、SoftLayer ポータルが変更されると変わる可能性があることに注意してください。この項ではあくまでも参考として示しています。

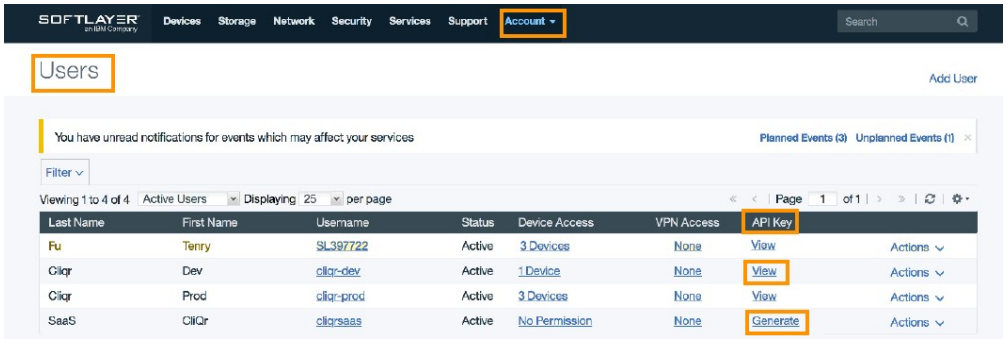
前提条件

CloudCenter プラットフォームで SoftLayer クラウドをマッピングする前に、次の SoftLayer 要件を確認します。

- 有効な SoftLayer PORTAL アカウント。
- **SoftLayer アカウント名**：SoftLayer ポータルの [Users] ページの [Username] 列に表示される正確な名前。必要なユーザ名をコピーして、以下の「*設定プロセス*」の説明に従って CloudCenter CCM UI で貼り付けます。



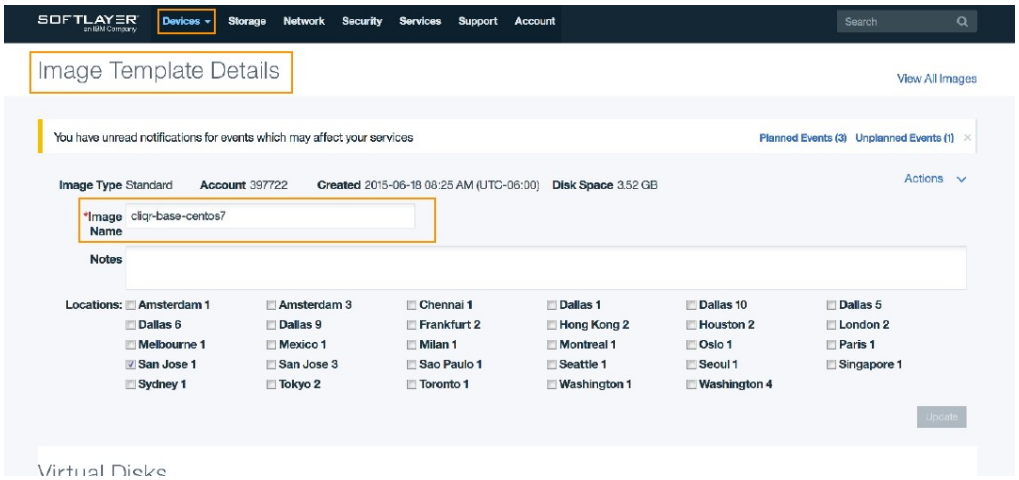
- **SoftLayer アカウント API キー**：これは、このユーザのアカウントの API キーです。このアカウントの API キーがない場合は、この時点で API キーを取得します。



  この API キーをコピーして、以下の「*設定プロセス*」の説明に従って CloudCenter CCM UI で貼り付けます。
  - すでに API キーが生成されている：SoftLayer ポータルの [Users] ページにアクセスします。（必要なユーザに対応する [API Key] 列で）[View] をクリックします。
  - API キーが生成されていない：SoftLayer ポータルの [Users] ページにアクセスします。（必要なユーザに対応する [API Key] 列で）[Generate] をクリックします。
- **デバイス名**：これは、SoftLayer ポータルの [Device List] ページの [Device Name] 列に表示される正確な名前です。必要なデバイス名をコピーして、以下の「*設定プロセス*」の説明に従って CloudCenter CCM UI で貼り付けます。

> この SoftLayer デバイスと同じクラウド リージョンで CCO を起動する必要があります。CCO とこのデバイスに異なるリージョンを選択することはできません。

- **イメージ**：これは、SoftLayer ポータルの [Images] ページの [Image Template Details] セクションに表示される正確な名前です。



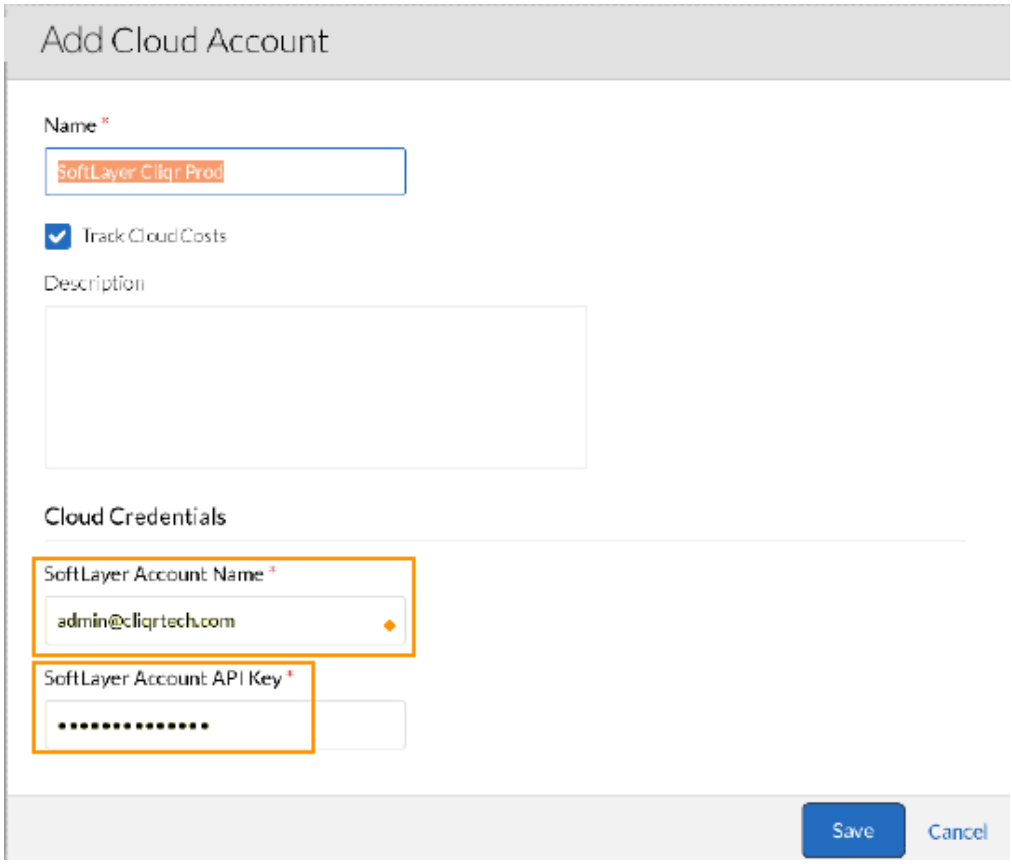
必要な**イメージ**名をコピーして、以下の「*設定プロセス*」の説明に従って CloudCenter CCM UI で貼り付けます。

設定プロセス

SoftLayer クラウドで論理マッピングを設定するには、次の手順に従います。

1. CCM UI にアクセスし、CCM UI のメインメニューで [管理（Admin）] > [クラウド（Clouds）] > [クラウドの追加（Add Cloud）] を選択します。

2. [SoftLayer an IBM Company] オプションを選択し、このクラウドの名前と説明を入力して、[保存（Save）] をクリックします。
3. 新たに追加されたクラウドを見つけて [クラウド アカウントの追加（Add Cloud Account）] リンクをクリックします。[クラウド アカウントの追加（Add Cloud Account）] ポップアップが表示されます。



a. 新しいクラウドに名前を割り当てます。

> **ヒント**
> 名前には、スペース、ダッシュ、特殊文字を含めることはできません。

b. SoftLayer アカウントに関連付けられている次のクラウド クレデンシャルを追加し、[保存(Save)] をクリックします。
   i. SoftLayer アカウント名(SoftLayer Account Name):上記「前提条件」セクションで説明している SoftLayer ユーザ名。
   ii. SoftLayer アカウント API キー(SoftLayerAccount API Key):上記「前提条件」セクションで説明している SoftLayer API キー。

4. [リージョン(Region)] タブをクリックし、クラウド リージョンを追加します。
   a. [クラウド リージョンの追加(Add Cloud Region)] をクリックします。
   b. このクラウドに必要なリージョンを選択します。
   c. このクラウド リージョンの [リージョン名(Region Name)] およびオプションの [表示名(Display Name)] を追加します。
   d. [保存(Save)] をクリックします。

> インスタンス タイプ、ストレージ タイプ、およびイメージ マップのセクションは、リージョンを追加するとすぐに自動的に設定されます。

5. [クラウド設定の編集(Edit Cloud Settings)] をクリックし、各リージョンの SoftLayer クラウド設定を更新します。
   a. **DefaultprivateVlanNumber**:この CloudCenter インスタンスを起動する必要があるデフォルトの SoftLayer プライベート クラウド ネットワークを指定します。
   b. **Default publicVlanNumber**:この CloudCenter インスタンスを起動する必要があるデフォルトの SoftLayer パブリック クラウド ネットワークを指定します。
   c. [保存(Save)] をクリックします。

> **注意**
> **クラウド設定を編集**する場合、変更を CCO に保存し、これらの変更がファイアウォールの設定内の CCO にも反映されるようにする必要があります。
>
> CCO がすでに設定されている場合は、これらのクラウド設定を有効にするために CCO を再登録する必要があります

6. クラウド設定を完了するには、CCO を CCM に登録する必要があります。
   CCM への CCO の登録

CCM への CCO の登録

- クラウド リージョンの微妙な違い
- 非 HA モード
- HA モード

クラウド リージョンの微妙な違い

CCM に CCO を登録すると、CCO は登録されたクラウド リージョンにのみ動作します。

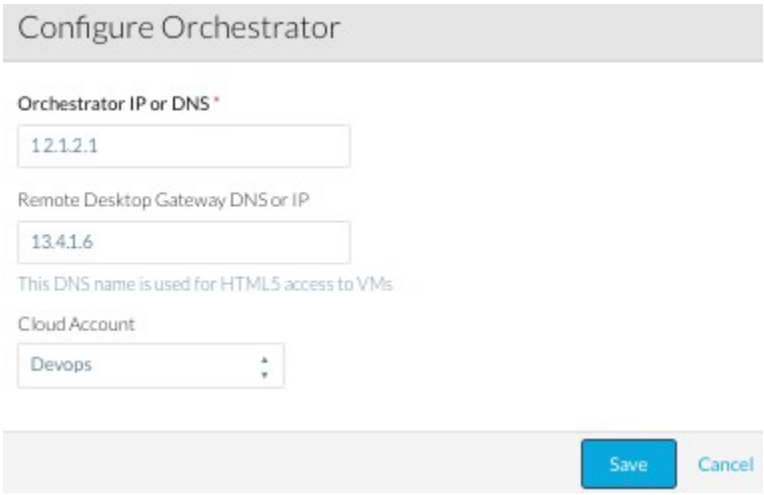
> **CloudCenter**
> CCM に CCO を登録すると、CloudCenter プラットフォームは、このクラウド リージョンがアクティブであると見なし、特定条件下でしか CloudCenter プラットフォームからこのクラウド リージョンを削除できなくなります。詳細については、「Cloud Region Configuration」>「*Delete Cloud Region*」を参照してください。

> 提供された例では AWS クラウドを参照していますが、スクリーン キャプチャはクラウドごとに異なることがある点に注意してください。

非 HA モード

CCM に CCO を登録するには、次の手順に従います。

a. [オーケストレータの設定（Configure Orchestrator）] ポップアップで、CCM からアクセス可能な CCO の IP アドレスを入力し、CCO をホストするために使用されるクラウド アカウントを選択します。



b. このページがまだ表示されていない場合は、必要なクラウドにおいて、[管理（Admin）] > [クラウド（Clouds）] > [リージョンの設定（Configure Regions）] を選択していることを確認します。
   i. [リージョン（Regions）] タブの [オーケストレータの設定（Configure Orchestrator）] をクリックします。
   ii. オーケストレータの IP または DNS（Orchestrator IP or DNS）：CCO サーバの IP または DNS アドレスを指定します。
   iii. リモート デスクトップ ゲートウェイの DNS または IP（Remote Desktop Gateway DNS or IP）：Guacamole サーバの IP アドレス（VM へのブラウザベースのアクセスを有効化）。Guacamole コンポーネントが AMQP サーバ内に存在している場合は、AMQP サーバの IP アドレスを指定します。
   iv. クラウド アカウント（Cloud Account）：この CCO で使用するクラウド アカウントを選択します。

> **Amazon クラウドの微妙な違い**
> IAM ロールを設定している場合、この設定は重要です。必ずこのロールを含むクラウド アカウントを選択してください。

c. [保存（Save）] をクリックします。これで、CCM と CCO の相互信頼関係が確立されました。CloudCenter プラットフォームは現在、導入された CCO によりクラウド リージョンを管理しています。
d. 手順 2 と手順 3 を繰り返し、CCM とその他の CCO 間の相互信頼を確立します。

CCO VM を登録し、設定が完了しました。ここでは、2 つのオプションがあります。

- その他のクラウド リージョンを追加し、これらのクラウドごとに CCO を登録します。詳細については、「クラウド リージョンごと（必須）」を参照してください。
- イメージをマッピングします。詳細については、「イメージ マッピング」を参照してください。

> クラウド アカウントのイメージを起動するアクセス許可を付与する必要がある場合は、「Image Launch Permissions」を参照してください。

- アプリケーションのモデリング、展開、および管理を行います。詳細については、「Application Profile」を参照してください。

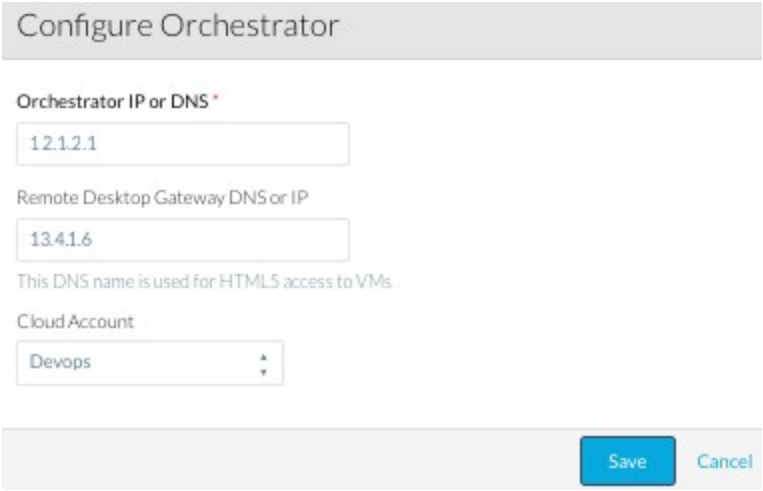
HA モード

CCM に CCO を登録するには、次の手順に従います。

a. プライマリ CCO で Tomcat Service が実行中であることを確認します。
b. セカンダリ CCO およびターシャリ CCO にログインし、両方のサーバで Tomcat Service を停止します。

```
/etc/init.d/tomcat stop
```

c. CCM UI にアクセスし、CCO LB の IP アドレスを使用して CCO を登録します。
   i. このページがまだ表示されていない場合は、必要なクラウドにおいて、[管理(Admin)] > [クラウド(Clouds)] > [リージョンの設定(Configure Regions)] を選択していることを確認します。
   ii. [リージョン(Regions)] タブの [オーケストレータの設定(Configure Orchestrator)] をクリックします。
   iii. CCM からアクセス可能な CCO の IP アドレスを入力し、CCO をホストするために使用されるクラウド アカウントを選択します。



      1. オーケストレータの IP または DNS(Orchestrator IP or DNS):CCO サーバの IP または DNS アドレスを指定します。
      2. リモート デスクトップ ゲートウェイの DNS または IP(Remote Desktop Gateway DNS or IP):Guacamole サーバの IP アドレス(VM へのブラウザベースのアクセスを有効化)。Guacamole コンポーネントが AMQP サーバ内に存在している場合は、AMQP サーバの IP アドレスを指定します。
      3. クラウド アカウント(Cloud Account):この CCO で使用するクラウド アカウントを選択します。必ずこのロールを含むクラウド アカウントを選択してください。
      4. [保存(Save)] をクリックします。これで、CCM と CCO の相互信頼関係が確立されました。CloudCenter プラットフォームは現在、導入された CCO によりクラウド リージョンを管理しています。

d. 登録が成功したら、プライマリ CCO サーバにログインします。
e. プライマリ CCO の **/usr/local/osmosix/etc/** フォルダから、セカンダリ CCO およびターシャリ CCO の両サーバ上の**同じ場所**に **gateway_config.properties** ファイルをコピーします。
f. すべてのサーバのコピーしたファイルの所有権およびアクセス許可が次のようになっていることを確認します。
   - オーナー(Owner)= cliqruser
   - グループ権限(Group Permission)= 読み取りおよび書き込み
g. 必要な場合は、次のコマンドを実行して設定を変更します。

```
chown
cliqruser:cliqruser
/usr/local/osmosix/etc/gateway_config.properties
chmod 644 /usr/local/osmosix/etc/gateway_config.properties
```

h. 各サーバで次のコマンドを発行することによって、セカンダリ CCO とターシャリ CCO サーバで Tomcat を起動します。

```
/etc/init.d/tomcat start
```

i. HA モードのその他の CCO についてこの手順を繰り返し、CCM とその他の CCO 間の相互信頼を確立します。

CCO VM を登録し、設定が完了しました。ここでは、2 つのオプションがあります。

- その他のクラウド リージョンを追加し、これらのクラウドごとに CCO を登録します。詳細については、「クラウド リージョンごと(必須)」を参照してください。
- イメージをマッピングします。詳細については、「イメージ マッピング」を参照してください。

> クラウド アカウントのイメージを起動するアクセス許可を付与する必要がある場合は、「Image Launch Permissions」を参照してください。

- アプリケーションのモデリング、展開、および管理を行います。詳細については、「Application Profile」を参照してください。

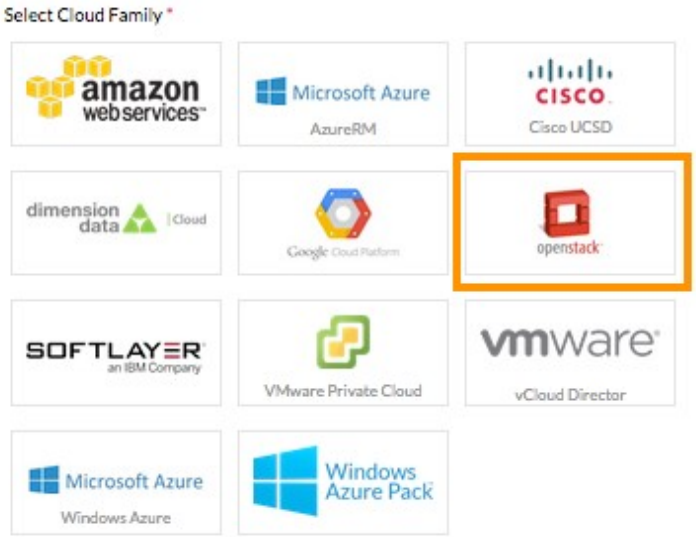
戻る:クラウドの設定

- OpenStack クラウドの設定

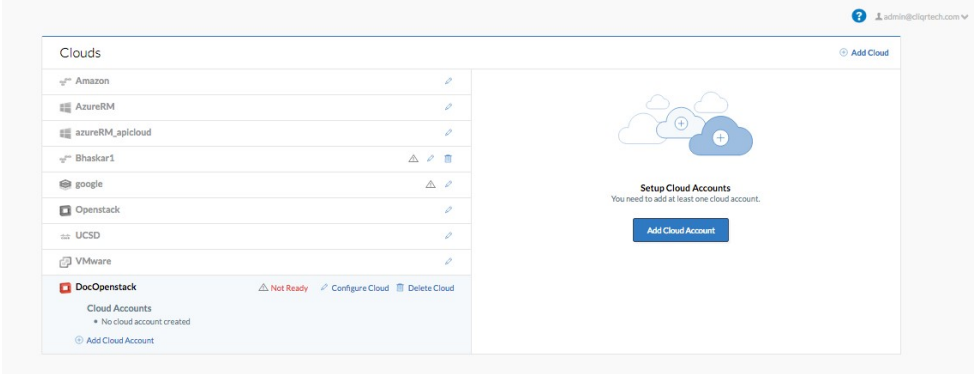
OpenStack クラウドの設定

OpenStack クラウドで論理マッピングを設定するには、次の手順に従います。

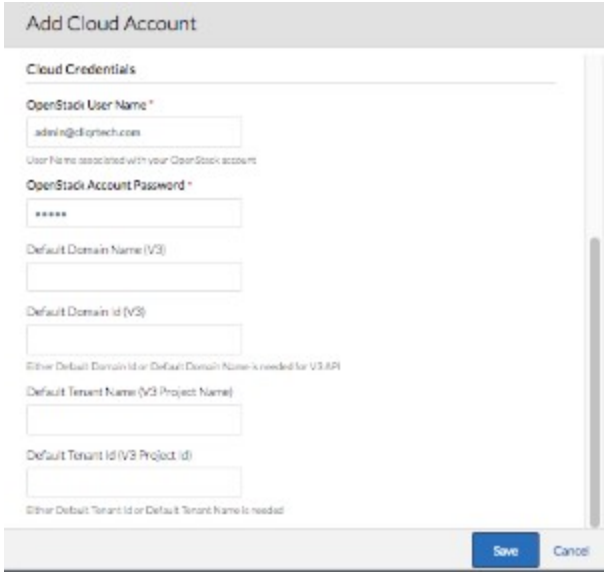
1. CCM UI にアクセスし、CCM UI のメインメニューで [管理(Admin)] > [クラウド(Clouds)] > [クラウドの追加(Add Cloud)] を選択します。



2. [OpenStack] を選択し、このクラウドの名前と説明を入力して、[保存(Save)] をクリックします。
3. 新たに追加されたクラウドを見つけて [クラウド アカウントの追加(Add Cloud Account)] をクリックし、このクラウド ファミリにアカウントを追加します。



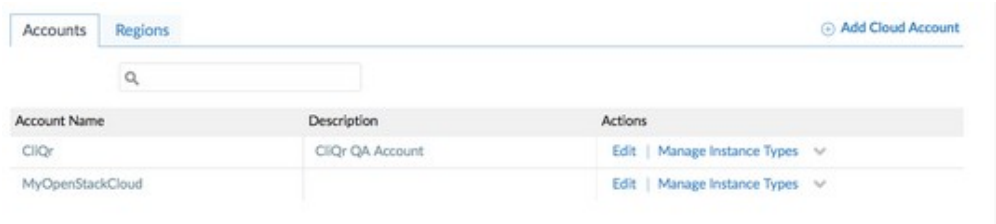
4. [クラウド アカウントの追加(Add Cloud Account)] をクリックして、このクラウド ファミリにアカウントを追加します。[クラウド アカウントの追加(Add Cloud Account)] ポップアップが表示されます。



OpenStack ユーザに完全な管理者権限がない場合は、(CloudCenter を使用する)各ユーザに少なくともアクセス権限があることを確認してください。

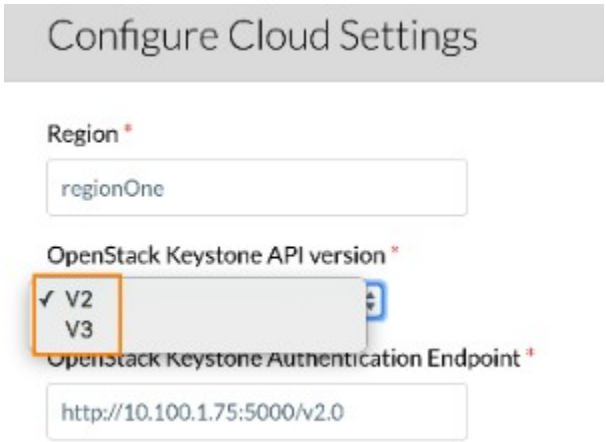
クラウド アカウントの詳細	説明
OpenStack ユーザ名/パスワード(OpenStack User Name/Password)	このクラウド アカウントにアクセスするためのクレデンシャル。
デフォルトドメイン名(V3)(Default Domain Name (V3))	これはオプションです。OpenStack クラウド アカウントの追加時には、V2 または V3 OpenStack エンドポイントを選択できます。 • V2 を使用する場合は必須ではありません。 • V3 を使用する場合は、デフォルトのドメイン ID またはデフォルトのドメイン名を入力します。 • クラウド リージョンの設定によりリージョンが検証されます。
デフォルトドメイン ID(V3)(Default Domain ID (V3))	
デフォルト テナント名(V3 プロジェクト名)(Default Tenant Name (V3 Project Name))	これはオプションです。OpenStack のプロジェクト名。
デフォルトドメイン ID(V3 プロジェクト ID)(Default Domain ID (V3 Project ID))	これはオプションです。設定すると、[デフォルト テナント ID(Default Tenant ID)](CloudCenter での OpenStack 設定)が [デフォルト テナント名(Default Tenant Name)] よりも優先されます。

a. 新しいクラウドに**名前**を割り当てます。
b. [クラウド コストの追跡(Track Cloud Costs)] チェックボックスをオンにして、クラウド コストを追跡します。
c. OpenStack のユーザ クレデンシャルを入力します。
d. これはオプションです。V3 API を使用する OpenStack ドメインを設定するには、ドメイン ID とドメイン名を追加します。V3 API ドメインを選択する場合は、ドメイン ID またはドメイン名を入力します。
e. [保存(Save)] をクリックし、新しく追加したクラウド アカウント(用語の詳細な説明は「Cloud」を参照)が [クラウド(Cloud)] ページに表示されていることを確認します。
f. [クラウドの設定(Configure Cloud)] リンクをクリックします。[クラウド アカウント(Cloud Accounts)] ページの [アカウント(Accounts)] タブに、設定したすべてのクラウド アカウントが表示されます。



5. [リージョン(Region)] タブをクリックし、クラウド リージョンを追加します。
   a. [クラウド リージョンの追加(Add Cloud Region)] をクリックします。
   b. このクラウドに必要なリージョンを選択します。
   c. このクラウド リージョンの [リージョン名(Region Name)] およびオプションの [表示名(Display Name)] を追加します。
   d. [保存(Save)] をクリックします。
6. [クラウド設定の編集(Edit Cloud Settings)] リンクをクリックし、各クラウド リージョンの設定を更新します。

- 必須の設定：
  - リージョン（Region）：（リージョンは有効な OpenStack リージョンにする必要があります）
  - OpenStack Keystone API バージョン（OpenStack Keystone API Version）：（ドロップダウン リストには、v2 と v3 の両方のオプションが含まれています。これらのオプションのいずれかを選択します）



  - OpenStack Keystone 認証エンドポイント（OpenStack Keystone Authentication Endpoint）：（この設定は [クラウド アカウント（Cloud Account）] ポップアップでは使用できません。[クラウド リージョン（Cloud Region）] ポップアップでのみ使用できます）
- オプション設定：[インスタンスの命名方法（Instance Naming Strategy）]、[インスタンス IPAM の使用（Instance IPAM Strategy）]、または [ノード名設定（Node Name Config）] フィールド。「VM Name Config」セクションでは、これらの値の設定の詳細を説明しています。

> **注意**
> **クラウド設定を編集**する場合、変更を CCO に保存し、これらの変更がファイアウォールの設定内の CCO にも反映されるようにする必要があります。
>
> CCO がすでに設定されている場合は、これらのクラウド設定を有効にするために CCO を再登録する必要があります。

7. クラウド設定を完了するには、CCO を CCM に登録する必要があります。
   CCM への CCO の登録

CCM への CCO の登録

- クラウド リージョンの微妙な違い
- 非 HA モード
- HA モード

クラウド リージョンの微妙な違い

CCM に CCO を登録すると、CCO は登録されたクラウド リージョンにのみ動作します。

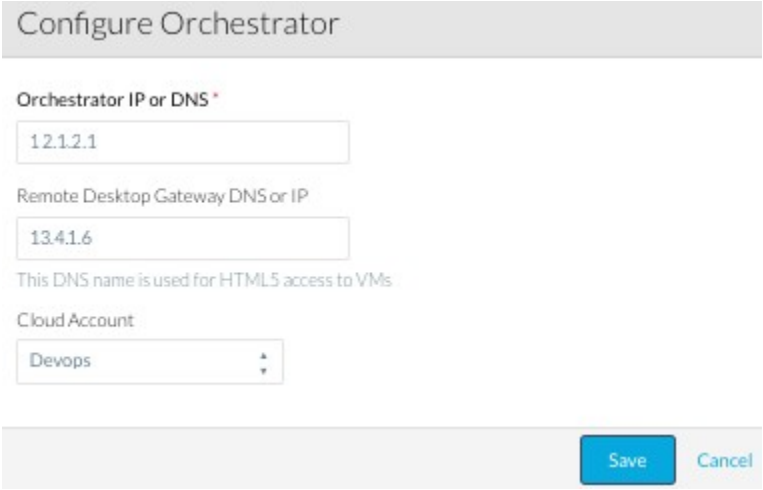
> **CloudCenter**
> CCM に CCO を登録すると、CloudCenter プラットフォームは、このクラウド リージョンがアクティブであると見なし、特定条件下でしか CloudCenter プラットフォームからこのクラウド リージョンを削除できなくなります。詳細については、「Cloud Region Configuration」>「*Delete Cloud Region*」を参照してください。

> 提供された例では AWS クラウドを参照していますが、スクリーン キャプチャはクラウドごとに異なることがある点に注意してください。

非 HA モード

CCM に CCO を登録するには、次の手順に従います。

a. [オーケストレータの設定（Configure Orchestrator）] ポップアップで、CCM からアクセス可能な CCO の IP アドレスを入力し、CCO をホストするために使用されるクラウド アカウントを選択します。



b. このページがまだ表示されていない場合は、必要なクラウドにおいて、[管理(Admin)] > [クラウド(Clouds)] > [リージョンの設定(Configure Regions)] を選択していることを確認します。
   i. [リージョン(Regions)] タブの [オーケストレータの設定(Configure Orchestrator)] をクリックします。
   ii. オーケストレータの IP または DNS(Orchestrator IP or DNS):CCO サーバの IP または DNS アドレスを指定します。
   iii. リモート デスクトップ ゲートウェイの DNS または IP(Remote Desktop Gateway DNS or IP):Guacamole サーバの IP アドレス(VM へのブラウザベースのアクセスを有効化)。Guacamole コンポーネントが AMQP サーバ内に存在している場合は、AMQP サーバの IP アドレスを指定します。
   iv. クラウド アカウント(Cloud Account):この CCO で使用するクラウド アカウントを選択します。

> **Amazon クラウドの微妙な違い**
> IAM ロールを設定している場合、この設定は重要です。必ずこのロールを含むクラウド アカウントを選択してください。

c. [保存(Save)] をクリックします。これで、CCM と CCO の相互信頼関係が確立されました。CloudCenter プラットフォームは現在、導入された CCO によりクラウド リージョンを管理しています。
d. 手順 2 と手順 3 を繰り返し、CCM とその他の CCO 間の相互信頼を確立します。

CCO VM を登録し、設定が完了しました。ここでは、2 つのオプションがあります。

- その他のクラウド リージョンを追加し、これらのクラウドごとに CCO を登録します。詳細については、「クラウド リージョンごと(必須)」を参照してください。
- イメージをマッピングします。詳細については、「イメージ マッピング」を参照してください。

> クラウド アカウントのイメージを起動するアクセス許可を付与する必要がある場合は、「Image Launch Permissions」を参照してください。

- アプリケーションのモデリング、展開、および管理を行います。詳細については、「Application Profile」を参照してください。

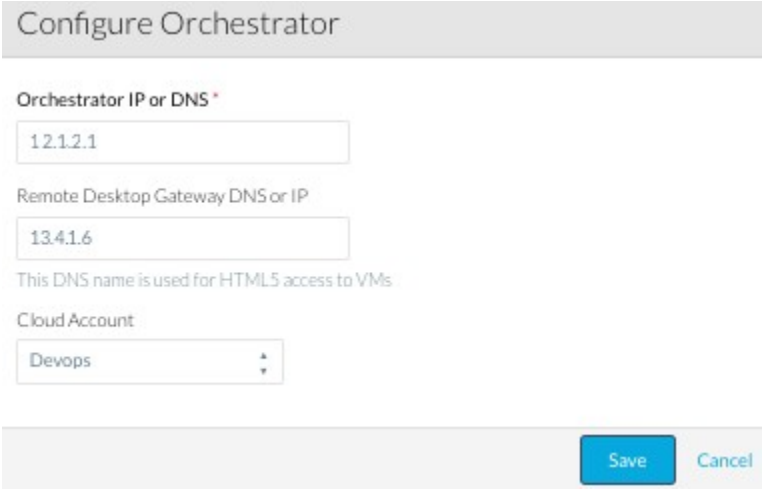
HA モード

CCM に CCO を登録するには、次の手順に従います。

a. プライマリ CCO で Tomcat Service が実行中であることを確認します。
b. セカンダリ CCO およびターシャリ CCO にログインし、両方のサーバで Tomcat Service を停止します。

```
/etc/init.d/tomcat stop
```

c. CCM UI にアクセスし、CCO LB の IP アドレスを使用して CCO を登録します。
   i. このページがまだ表示されていない場合は、必要なクラウドにおいて、[管理(Admin)] > [クラウド(Clouds)] > [リージョンの設定(Configure Regions)] を選択していることを確認します。
   ii. [リージョン(Regions)] タブの [オーケストレータの設定(Configure Orchestrator)] をクリックします。
   iii. CCM からアクセス可能な CCO の IP アドレスを入力し、CCO をホストするために使用されるクラウド アカウントを選択します。



1. オーケストレータの IP または DNS（Orchestrator IP or DNS）：CCO サーバの IP または DNS アドレスを指定します。
2. リモート デスクトップ ゲートウェイの DNS または IP（Remote Desktop Gateway DNS or IP）：Guacamole サーバの IP アドレス（VM へのブラウザベースのアクセスを有効化）。Guacamole コンポーネントが AMQP サーバ内に存在している場合は、AMQP サーバの IP アドレスを指定します。
3. クラウド アカウント（Cloud Account）：この CCO で使用するクラウド アカウントを選択します。必ずこのロールを含むクラウド アカウントを選択してください。
4. [保存（Save）] をクリックします。これで、CCM と CCO の相互信頼関係が確立されました。CloudCenter プラットフォームは現在、導入された CCO によりクラウド リージョンを管理しています。

d. 登録が成功したら、プライマリ CCO サーバにログインします。
e. プライマリ CCO の **/usr/local/osmosix/etc/** フォルダから、セカンダリ CCO およびターシャリ CCO の両サーバ上の**同じ場所**に **gateway_config.properties** ファイルをコピーします。
f. すべてのサーバのコピーしたファイルの所有権およびアクセス許可が次のようになっていることを確認します。
   - オーナー（Owner）= cliqruser
   - グループ権限（Group Permission）= 読み取りおよび書き込み
g. 必要な場合は、次のコマンドを実行して設定を変更します。

```
chown
cliqruser:cliqruser
/usr/local/osmosix/etc/gateway_config.properties
chmod 644 /usr/local/osmosix/etc/gateway_config.properties
```

h. 各サーバで次のコマンドを発行することによって、セカンダリ CCO とターシャリ CCO サーバで Tomcat を起動します。

```
/etc/init.d/tomcat start
```

i. HA モードのその他の CCO についてこの手順を繰り返し、CCM とその他の CCO 間の相互信頼を確立します。

CCO VM を登録し、設定が完了しました。ここでは、2 つのオプションがあります。

- その他のクラウド リージョンを追加し、これらのクラウドごとに CCO を登録します。詳細については、「クラウド リージョンごと（必須）」を参照してください。
- イメージをマッピングします。詳細については、「イメージ マッピング」を参照してください。

> クラウド アカウントのイメージを起動するアクセス許可を付与する必要がある場合は、「Image Launch Permissions」を参照してください。

- アプリケーションのモデリング、展開、および管理を行います。詳細については、「Application Profile」を参照してください。

戻る：クラウドの設定

- Google Cloud の設定

Google Cloud の設定

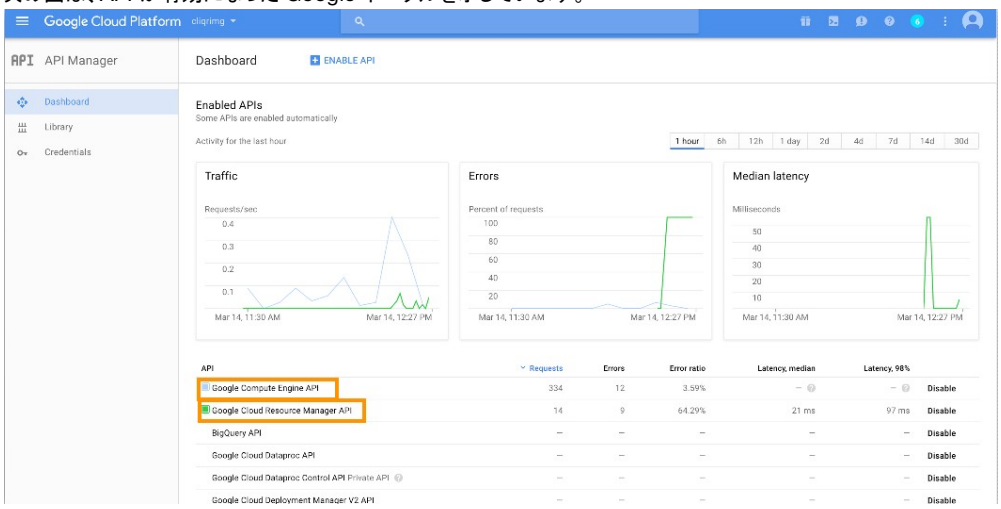
> 次のスクリーン キャプチャは、Google Cloud プラットフォームが変更されると変わる可能性があることに注意してください。この項ではあくまでも参考として示しています。

前提条件

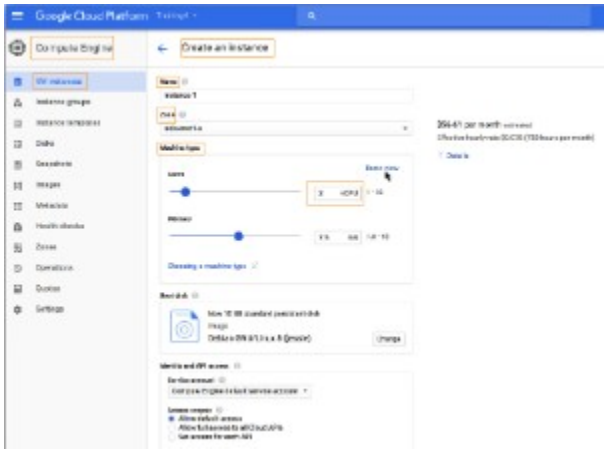
CloudCenter プラットフォームで Google クラウドをマッピングする前に、次の Google 要件を確認します。

- *プロジェクト所有者*のアクセス許可がある有効な Google Cloud Platform アカウント
- XPN ネットワーク機能を使用する場合、XPN Admin のアクセス許可も必要です（詳細については、https://cloud.google.com/compute/docs/xp n/provisioning-xpn を参照）。
- CloudCenter プラットフォームに追加する Google クラウド アカウントごとに次の API を有効にします。
  - Google Compute Engine API
  - Google Cloud Resource Manager API

  次の図は、API が有効になった Google ポータルを示しています。



- Google クラウドと同じクラウド リージョンで CCO を起動し、Google Cloud Platform コンソールで Google クラウドのインスタンスを作成します。

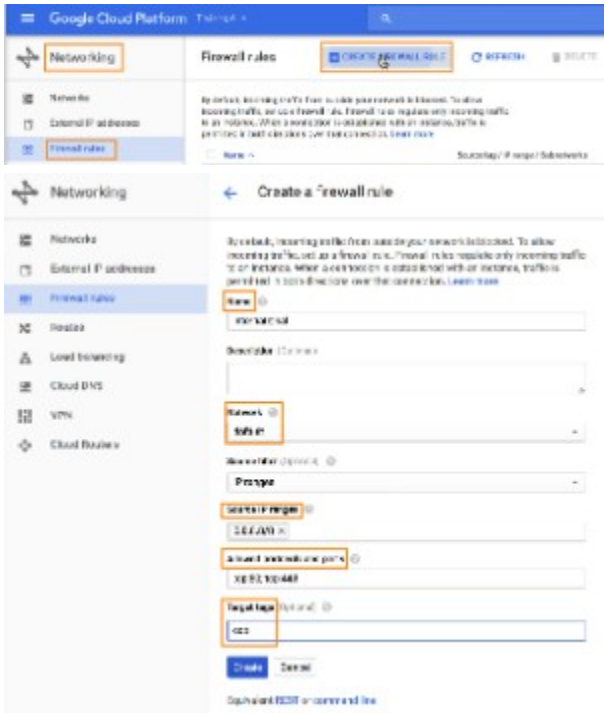


  - [Boot Disk] フィールドで OS イメージとして CentOS7 を選択し、必要に応じてディスクの**サイズ**を増やします（詳細については、「フェーズ 1：インフラストラクチャの準備」>「*ハードウェア要件*」を参照）。
  - 新しく作成されたインスタンスにアクセスし、編集して [Custom metadata] を追加します。

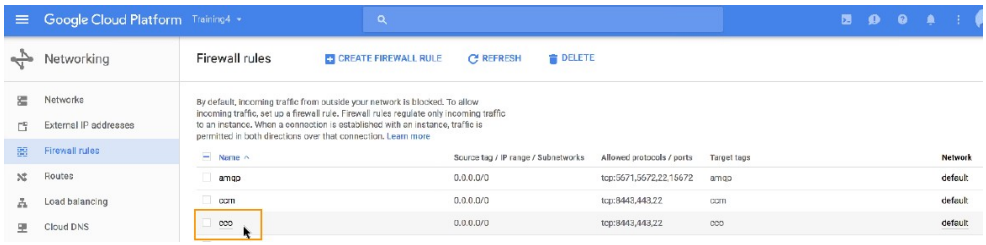
    カスタム メタデータの詳細

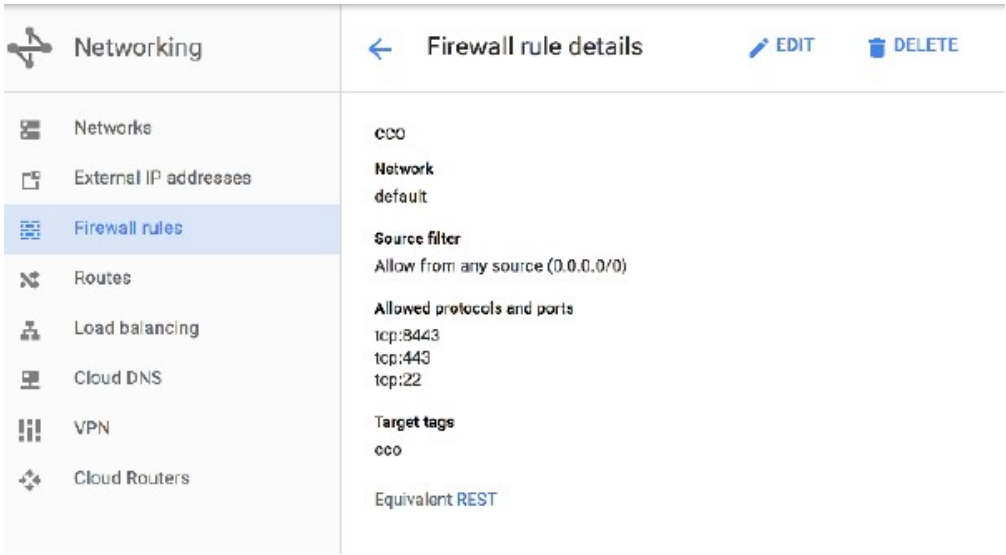
    sourceImageKey を追加し、任意の名前を指定します。

- Google Cloud Platform で次の画面に移動します。

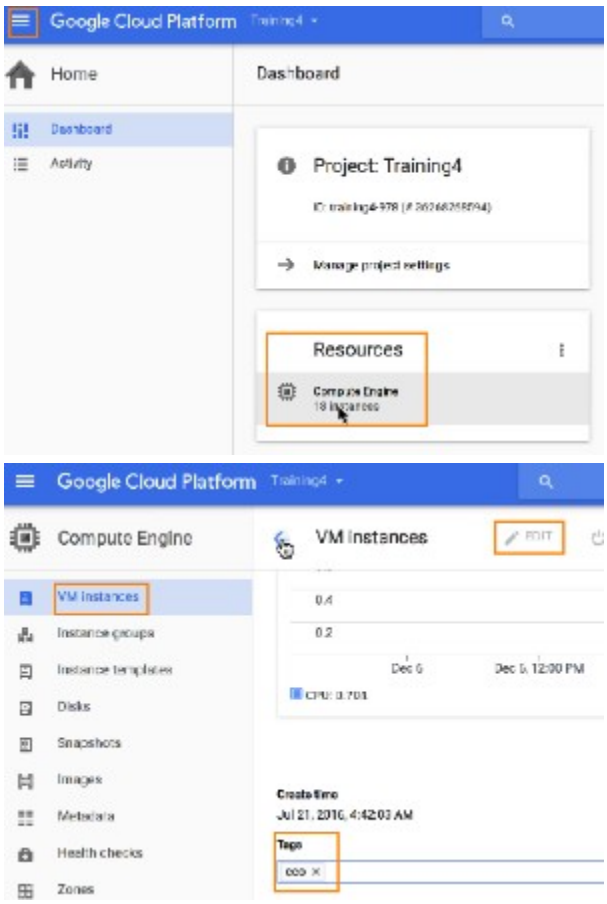


  - Name：必要に応じて任意の名前を指定します。
  - Network：デフォルト（CloudCenter ではこのフィールドのカスタム ネットワークがサポートされません）。
  - Source IP ranges：0.0.0.0/0（これは例です。環境の必要に応じてセキュアな IP 範囲を指定してください）。
  - Allowed protocols and ports：tcp:80;tcp:443（これは例です。環境のポートとプロトコルを指定してください）。
  - Target Tags：このフィールドは、CloudCenter の設定では必須です。CCO インスタンスを起動している場合は、タグとして **cco** を追加します。
  - 新しく作成されたファイアウォール ルールを作成し、リストに追加されていることを確認します。

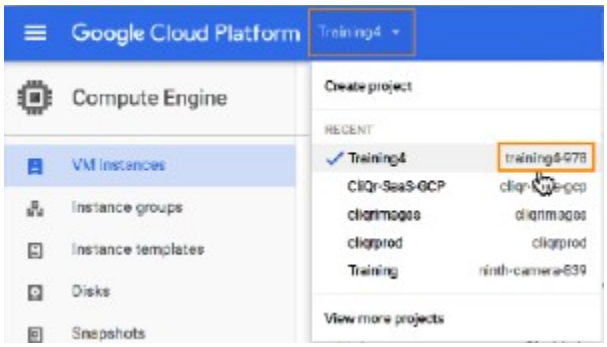




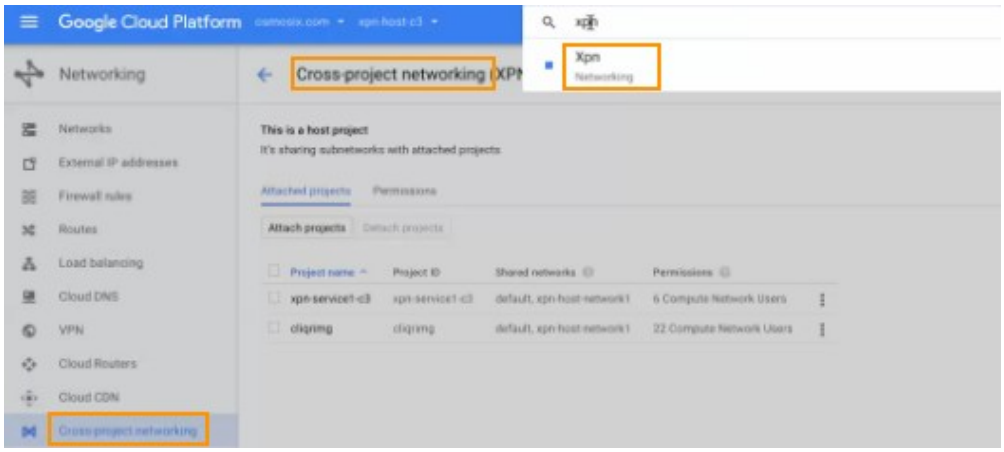
- [Compute Engine] ダッシュボードで、起動した VM インスタンスにアクセスし、ファイアウォール ルール タグ（この例の **cco**）をこの VM インスタンスに適用します。



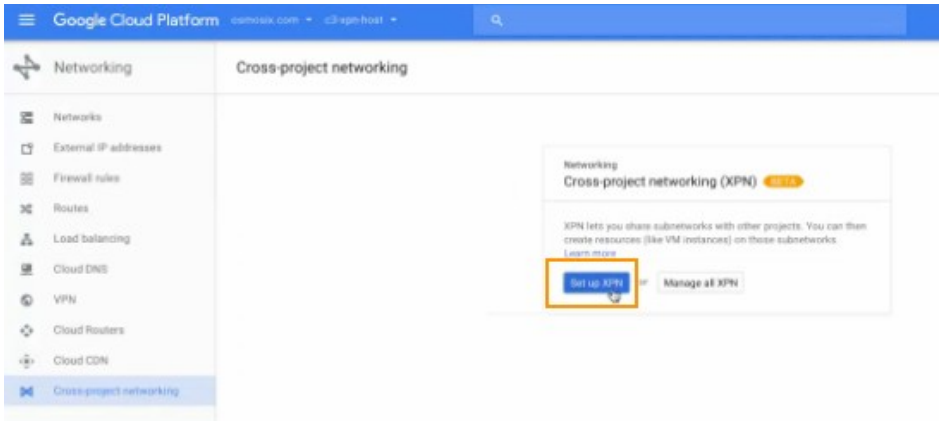
- **GCP プロジェクト ID**：これは、GCP へのログインに使用するアカウントに関連付けられているプロジェクト ID です。



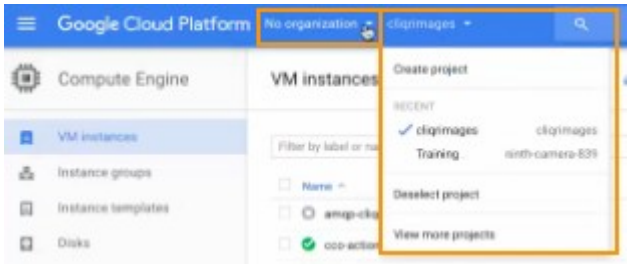
CloudCenter 4.7.3 では、CloudCenter プラットフォームで Google のベータ版のクロス プロジェクト ネットワーク（XPN）機能が追加でサポートされるようになりました。この機能では、同じネットワーク上の複数のプロジェクトを共有できます。XPN サポートの一般的な使用例は、同じネットワーク上で複数の部門が独自のプロジェクトを持っている場合です。この使用例では、1 つの部門が *XPN ホスト プロジェクト*とネットワークを作成し、他の部門とネットワークを共有します（*XPN サービス プロジェクト*）。

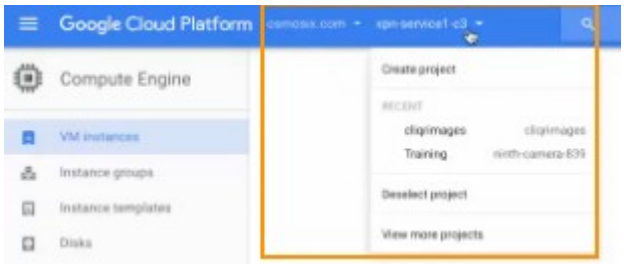


- CloudCenter プラットフォームでは、*XPN ホスト プロジェクト*のために GCP で次の設定が必要です。GCP プロ
  - ジェクトのいずれかを XPN プロジェクトとしてセットアップします。

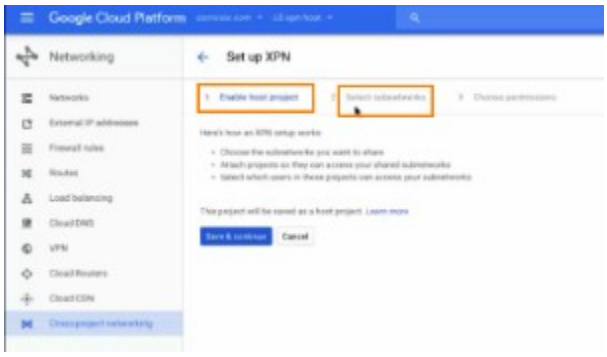


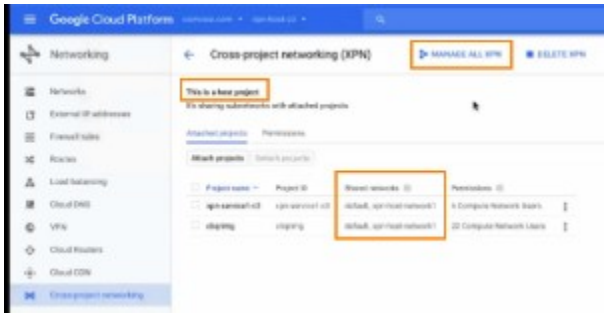
  - XPN プロジェクトは*組織内*にある必要があります（右の画像に表示されます）。



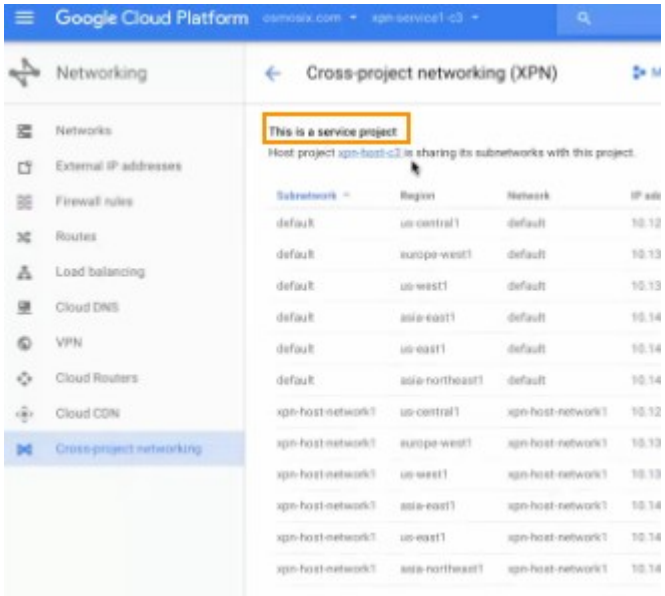


- プロジェクトは XPN ホストとして有効にする必要があり、共有サブネットワークを割り当てる必要があります。





- サービス プロジェクトは、共有サブネットワークを表示する必要があります。

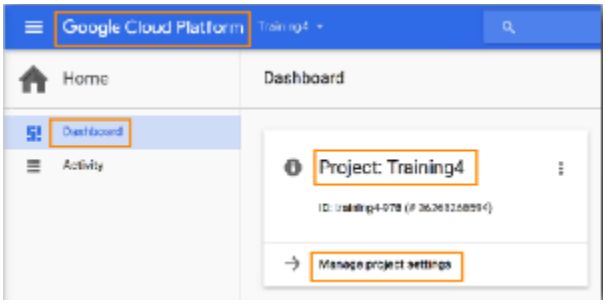


- **GCP サービス アカウントの電子メールアドレス**:このプロジェクトに関連付けられているサービス アカウントの電子メールアドレス。

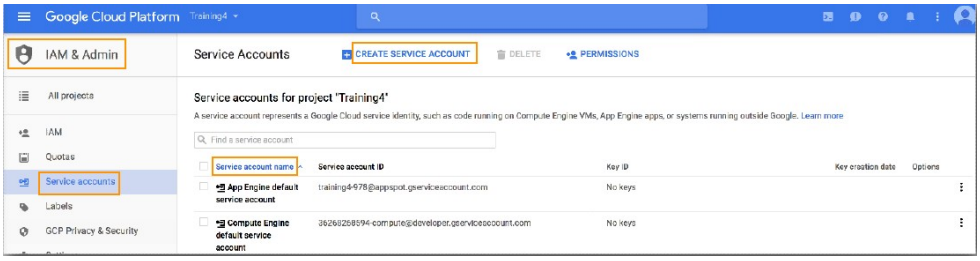
  電子メールアドレスの取得

  電子メールアドレスを取得するには、次の手順に従います。

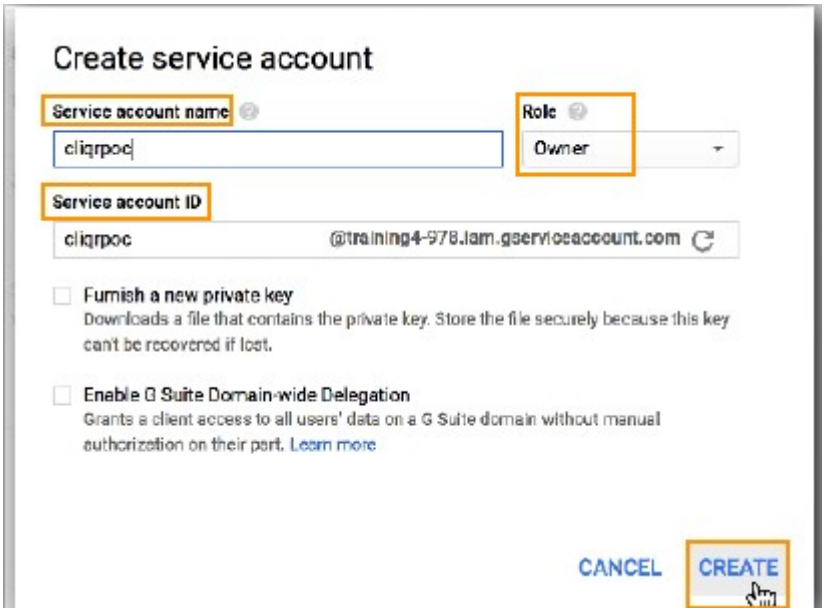
  - Google Cloud Platform の [Manage project settings] 画面に移動します。



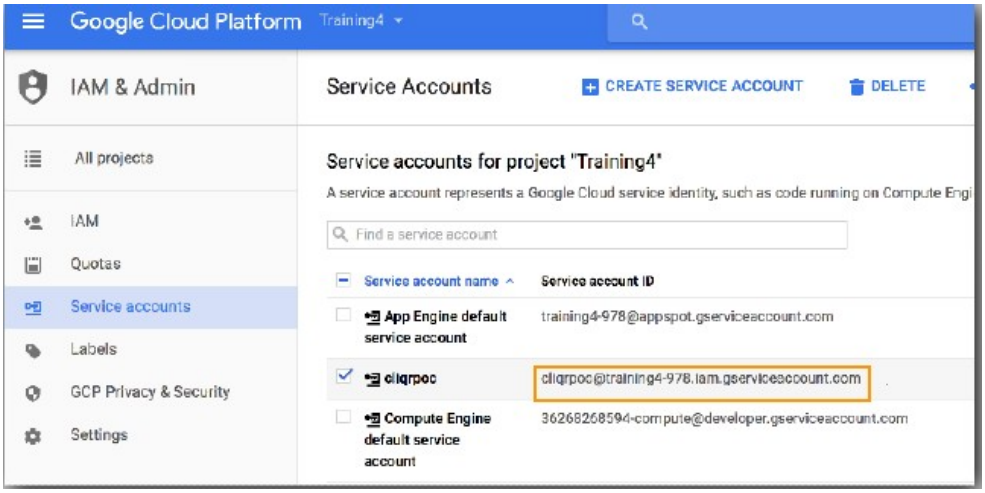
- [IAM & Admin] セクションで必要なサービス アカウント名を探します。



- 既存のサービス アカウントがない場合は、ここで作成します（このアカウントのロールを選択するときは、[Owner] を選択し、すべてのリソースへのフル アクセスがあることを確認します）。



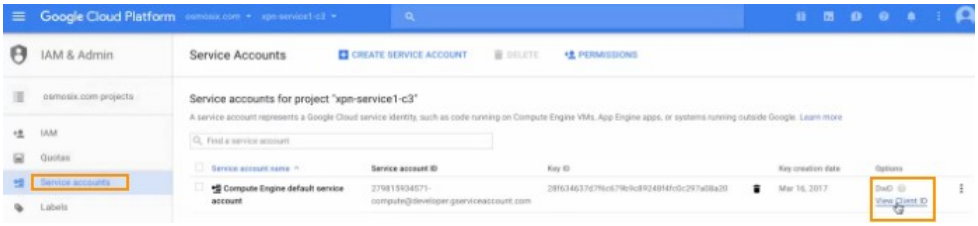
- 次の図で強調表示されているようにサービス アカウント ID を特定します。このサービス アカウント ID は、CCM UI の [GCP サービス アカウントの電子メールアドレス（GCP Service Account）] フィールドに必要です。



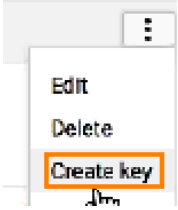
- **GCP サービス アカウント PK ファイル名**：この時点で新しいキーを作成し、このキーは再度表示されないため、**コピーします**。P12 ファイルのこの新しい名前は、CCM UI の [GCP サービス アカウント PK ファイル名（GCP Service Account PK Filename）] フィールドに必要です。

  GCP サービス アカウント PK ファイル名参照

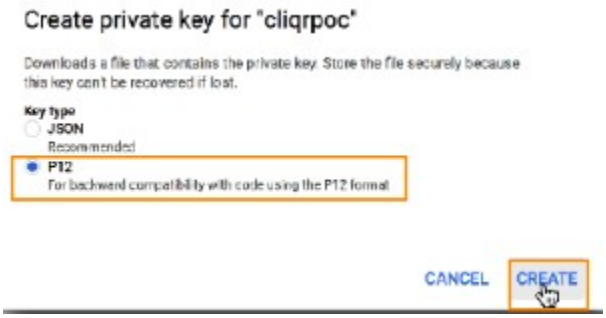
  - [IAM & Admin] ページから、上記で設定したサービス アカウントを見つけます。



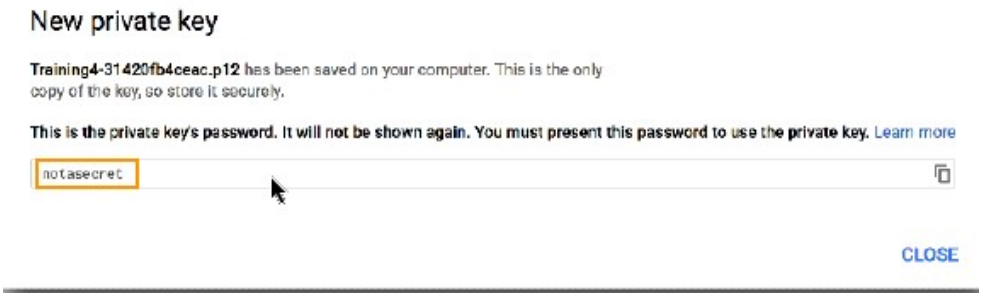
  - すでに作成されている場合は、キーを取得します。作成されていない場合は、このサービス アカウント ID に対応するアイコンをクリックし、[Create Key] オプションを選択します。



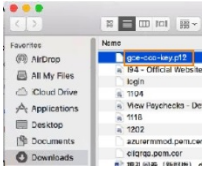
  - このキーのファイル形式を [P12] に変更し、この秘密キーのファイルを作成します。



  - このファイルに自動的に割り当てられた名前をメモします。メモに書き留めない場合、新しいキーの作成が必要になることがあります。



  - 簡単に参照できるようにダウンロード場所でこのファイルの名前を変更します。



- 上記の前提条件に基づいて次の詳細をメモし、これらを以下の「*設定プロセス*」で指定されたとおりに CCM UI に入力しやすいようにします。これらの詳細は、プロジェクトが単一プロジェクトか XPN プロジェクトかによって異なります。
  - **GCP 電子メールアドレス**（GCP へのログインに使用される電子メール）
  - **GCP サービス アカウントの電子メールアドレス**（このプロジェクトのサービス アカウント ID）

> XPN ホスト プロジェクトから共有ネットワークを使用する場合、必ず次の Google 固有のロール（*Compute Security Admin* ロールおよび *Compute Network User* ロール）を XPN ホスト プロジェクトのサービス アカウントに追加します。両方のロールが必須です。

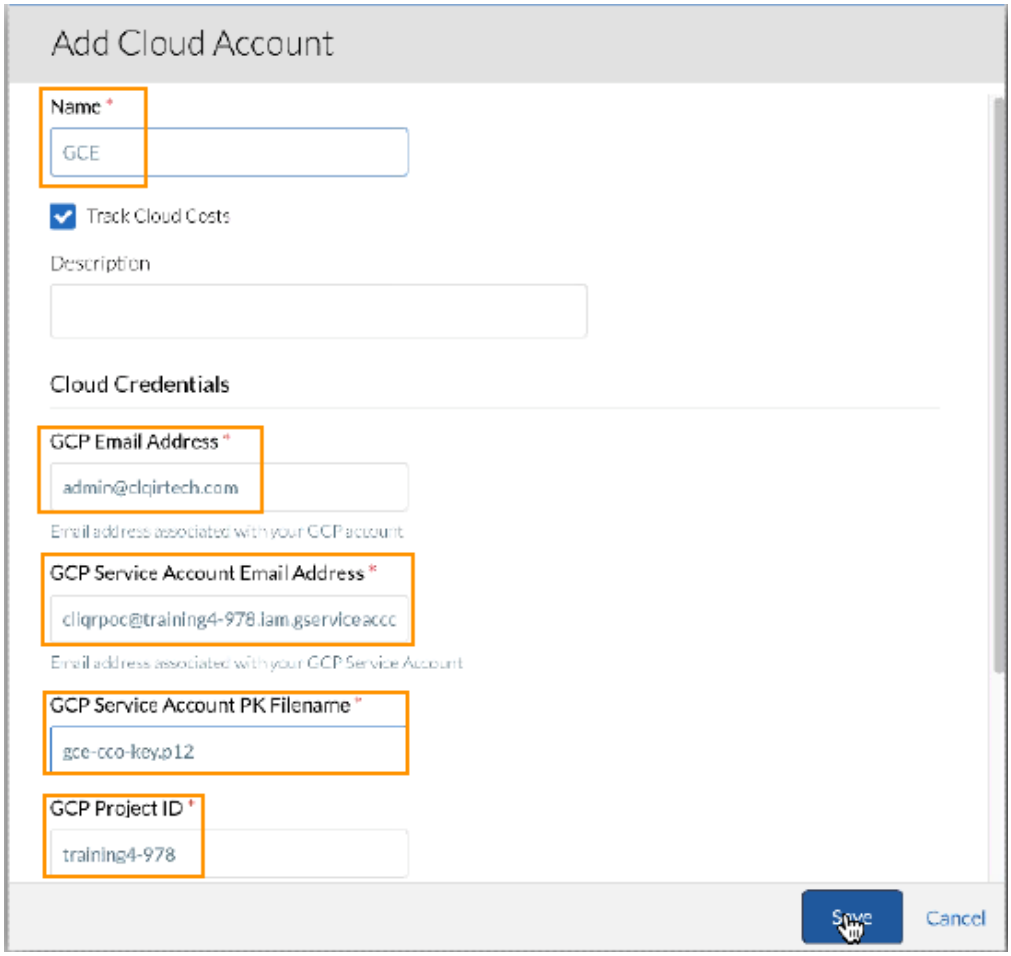
- このアカウントの **GCP プロジェクト ID**（このアカウントのプロジェクト ID）
- **GCP サービス アカウント PK ファイル名**（ダウンロードしたキー ファイルの名前）

設定プロセス

Google クラウドで論理マッピングを設定するには、次の手順に従います。

1. CCM UI にアクセスし、CCM UI のメインメニューで [管理（Admin）] > [クラウド（Clouds）] > [クラウドの追加（Add Cloud）] を選択します。

2. [Google Cloud Platform] オプションを選択し、このクラウドの名前と説明を入力して、[保存（Save）] をクリックします。
3. 新たに追加されたクラウドを見つけて [クラウド アカウントの追加（Add Cloud Account）] リンクをクリックします。[クラウド アカウントの追加（Add Cloud Account）] ポップアップが表示されます。



a. 新しいクラウドに名前を割り当てます。

> **ヒント**
> 名前には、スペース、ダッシュ、特殊文字を含めることはできません。

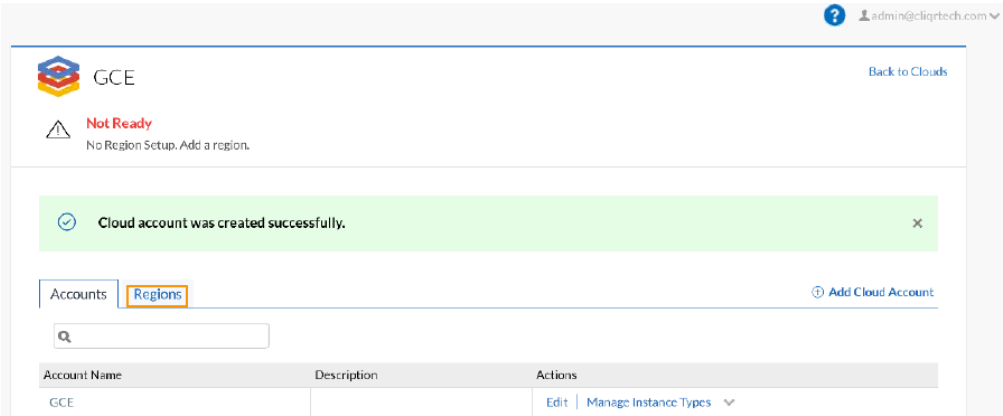
b. Google アカウントに関連付けられている次のクラウド クレデンシャルを追加し、[保存(Save)] をクリックします。

> これらの詳細は、プロジェクトが単一プロジェクトか共有 XPN プロジェクトかによって異なります。

GCP のこれらの詳細の場所は、上記の「*前提条件*」セクションで特定されます

フィールド	説明(CloudCenter 4.7.2x 以前)	XPN プロジェクトの微妙な違い(CloudCenter 4.7.3)
GCP 電子メールアドレス(GCP Email Address)	GCP アカウントへのログインに使用した電子メールアドレス。	
GCP サービス アカウントの電子メールアドレス(GCP Service Account Email Address)	Google API キー。	XPN プロジェクトに関連付けられている Google API キー。
GCP サービス アカウント PK ファイル名(GCP Service Account PK File Name)	P12 キー ファイルの名前。	XPN プロジェクトに関連付けられている P12 キー。
GCP プロジェクト ID(GCP Project ID)	GCP へのログインに使用したアカウントに関連付けられている ID。	XPN プロジェクトに関連付けられている ID。
ユーザ ネットワーク(User Network)	この省略可能なフィールドでは、Google ユーザ ネットワークの詳細を特定でき、クラウドの設定には影響しません。	未使用。

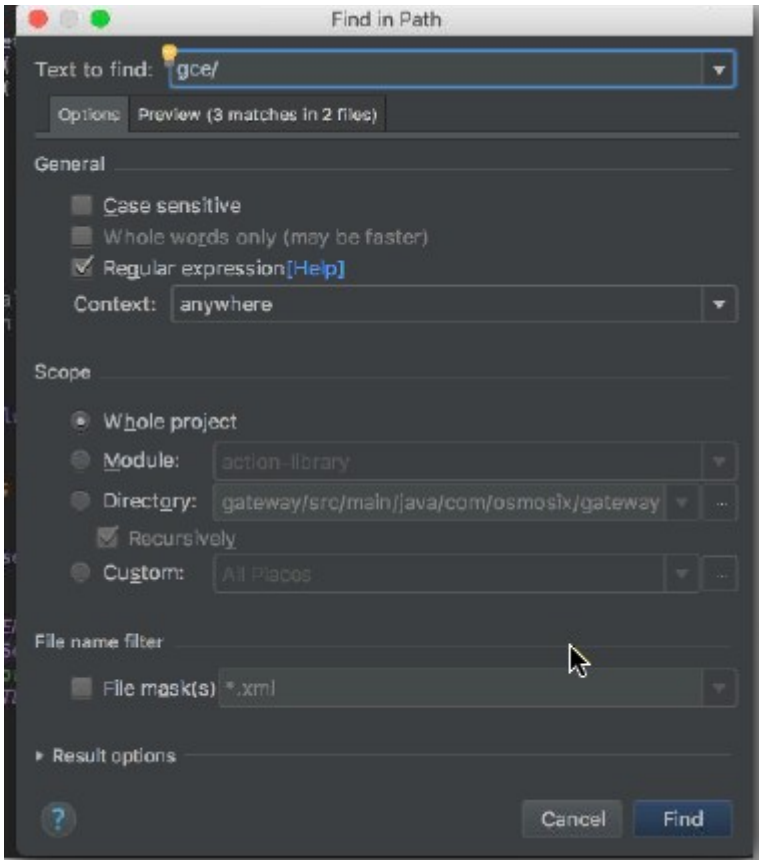
4. [リージョン(Regions)] タブをクリックします。



5. 新しいリージョンを追加する前に、CCO インスタンスにも Google Cloud Platform キーを追加する必要があります。

> この手順は重要です。Google Cloud Platform クラウドにアカウントを追加するたびに、Google Cloud Platform のそのアカウントに対して新しいキーを作成し、この時点で CCO インスタンスに P12 キーを追加してからリージョンを設定する必要があります。

a. CCO サーバにアクセスし、Google Cloud Platform のキー パスの場所を検索します。



b. 次のパスの末尾に Google Cloud Platform P12 キー ファイルの名前を挿入します。
/usr/local/osmosix/gce/keys/***addKeyFile Namehere***

例 : **/usr/local/osmosix/gce/keys/gce-cco-key.p12**

6. [リージョン（Region）] タブをクリックし、クラウド リージョンを追加します。
   a. [クラウド リージョンの追加（Add Cloud Region）] をクリックします。
   b. このクラウドに必要なリージョンを選択します。
   c. このクラウド リージョンの [リージョン名（Region Name）] およびオプションの [表示名（Display Name）] を追加します。
   d. [保存（Save）] をクリックします。

> インスタンス タイプ、ストレージ タイプ、およびイメージ マップのセクションは、リージョンを追加するとすぐに自動的に設定されます。

7. [クラウド設定の編集（Edit Cloud Settings）] をクリックし、各リージョンの Google クラウド設定を更新します。

> **注意**
> **クラウド設定を編集**する場合、変更を CCO に保存し、これらの変更がファイアウォールの設定内の CCO にも反映されるようにする必要があります。
>
> CCO がすでに設定されている場合は、これらのクラウド設定を有効にするために CCO を再登録する必要があります。

   a. 各プロジェクトには独自のクレデンシャルがあり、これらの設定はプロジェクト間で異なる場合があるため、プロジェクトごとにクラウド クレデンシャルを割り当てます。これらのフィールドは、すでに上記の手順 3 で説明しています。
   b. [保存（Save）] をクリックします。
8. クラウド設定を完了するには、CCO を CCM に登録する必要があります。
   CCM への CCO の登録

CCM への CCO の登録

- クラウド リージョンの微妙な違い
- 非 HA モード
- HA モード

クラウド リージョンの微妙な違い

CCM に CCO を登録すると、CCO は登録されたクラウド リージョンにのみ動作します。

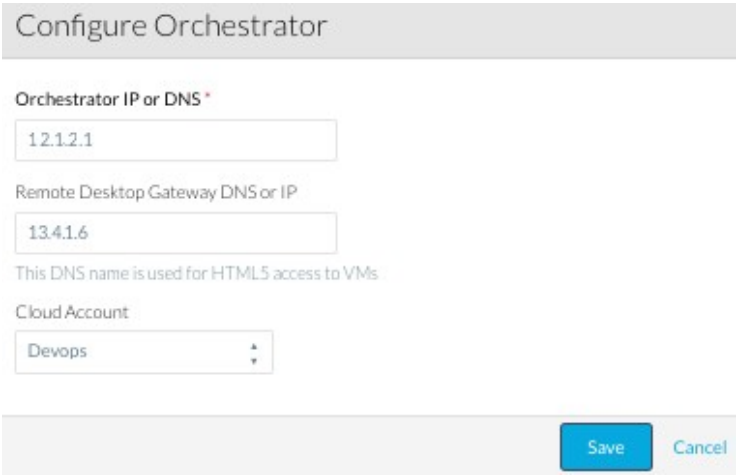
> **CloudCenter**
> CCM に CCO を登録すると、CloudCenter プラットフォームは、このクラウド リージョンがアクティブであると見なし、特定条件下でしか CloudCenter プラットフォームからこのクラウド リージョンを削除できなくなります。詳細については、「Cloud Region Configuration」>「*Delete Cloud Region*」を参照してください。

> 提供された例では AWS クラウドを参照していますが、スクリーン キャプチャはクラウドごとに異なることがある点に注意してください。

非 HA モード

CCM に CCO を登録するには、次の手順に従います。

a. [オーケストレータの設定（Configure Orchestrator）] ポップアップで、CCM からアクセス可能な CCO の IP アドレスを入力し、CCO をホストするために使用されるクラウド アカウントを選択します。



b. このページがまだ表示されていない場合は、必要なクラウドにおいて、[管理（Admin）] > [クラウド（Clouds）] > [リージョンの設定（Configure Regions）] を選択していることを確認します。
   i. [リージョン（Regions）] タブの [オーケストレータの設定（Configure Orchestrator）] をクリックします。
   ii. オーケストレータの IP または DNS（Orchestrator IP or DNS）：CCO サーバの IP または DNS アドレスを指定します。
   iii. リモート デスクトップ ゲートウェイの DNS または IP（Remote Desktop Gateway DNS or IP）：Guacamole サーバの IP アドレス（VM へのブラウザベースのアクセスを有効化）。Guacamole コンポーネントが AMQP サーバ内に存在している場合は、AMQP サーバの IP アドレスを指定します。
   iv. クラウド アカウント（Cloud Account）：この CCO で使用するクラウド アカウントを選択します。

> **Amazon クラウドの微妙な違い**
> IAM ロールを設定している場合、この設定は重要です。必ずこのロールを含むクラウド アカウントを選択してください。

c. [保存（Save）] をクリックします。これで、CCM と CCO の相互信頼関係が確立されました。CloudCenter プラットフォームは現在、導入された CCO によりクラウド リージョンを管理しています。
d. 手順 2 と手順 3 を繰り返し、CCM とその他の CCO 間の相互信頼を確立します。

CCO VM を登録し、設定が完了しました。ここでは、2 つのオプションがあります。

- その他のクラウド リージョンを追加し、これらのクラウドごとに CCO を登録します。詳細については、「クラウド リージョンごと（必須）」を参照してください。
- イメージをマッピングします。詳細については、「イメージ マッピング」を参照してください。

> クラウド アカウントのイメージを起動するアクセス許可を付与する必要がある場合は、「Image Launch Permissions」を参照してください。

- アプリケーションのモデリング、展開、および管理を行います。詳細については、「Application Profile」を参照してください。

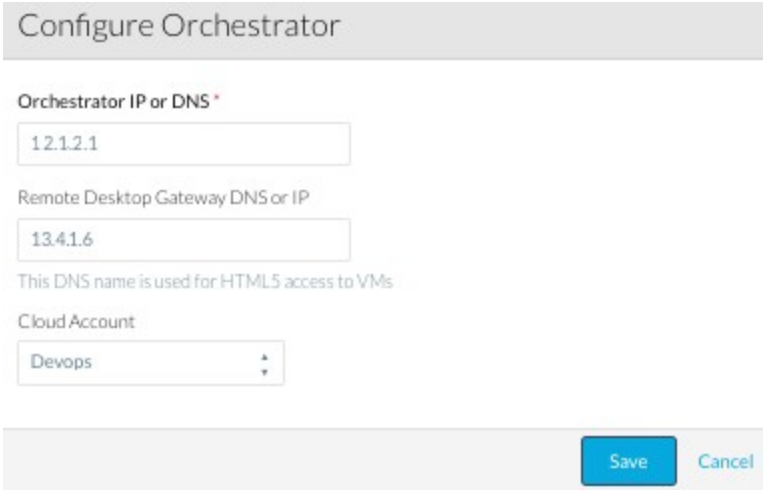
HA モード

CCM に CCO を登録するには、次の手順に従います。

a. プライマリ CCO で Tomcat Service が実行中であることを確認します。
b. セカンダリ CCO およびターシャリ CCO にログインし、両方のサーバで Tomcat Service を停止します。

```
/etc/init.d/tomcat stop
```

c. CCM UI にアクセスし、CCO LB の IP アドレスを使用して CCO を登録します。
   i. このページがまだ表示されていない場合は、必要なクラウドにおいて、[管理(Admin)] > [クラウド(Clouds)] > [リージョンの設定(Configure Regions)] を選択していることを確認します。
   ii. [リージョン(Regions)] タブの [オーケストレータの設定(Configure Orchestrator)] をクリックします。
   iii. CCM からアクセス可能な CCO の IP アドレスを入力し、CCO をホストするために使用されるクラウド アカウントを選択します。



   1. オーケストレータの IP または DNS(Orchestrator IP or DNS):CCO サーバの IP または DNS アドレスを指定します。
   2. リモート デスクトップ ゲートウェイの DNS または IP(Remote Desktop Gateway DNS or IP):Guacamole サーバの IP アドレス(VM へのブラウザベースのアクセスを有効化)。Guacamole コンポーネントが AMQP サーバ内に存在している場合は、AMQP サーバの IP アドレスを指定します。
   3. クラウド アカウント(Cloud Account):この CCO で使用するクラウド アカウントを選択します。必ずこのロールを含むクラウド アカウントを選択してください。
   4. [保存(Save)] をクリックします。これで、CCM と CCO の相互信頼関係が確立されました。CloudCenter プラットフォームは現在、導入された CCO によりクラウド リージョンを管理しています。

d. 登録が成功したら、プライマリ CCO サーバにログインします。
e. プライマリ CCO の **/usr/local/osmosix/etc/** フォルダから、セカンダリ CCO およびターシャリ CCO の両サーバ上の**同じ場所**に **gateway_config.properties** ファイルをコピーします。
f. すべてのサーバのコピーしたファイルの所有権およびアクセス許可が次のようになっていることを確認します。
   - オーナー(Owner)= cliqruser
   - グループ権限(Group Permission)= 読み取りおよび書き込み
g. 必要な場合は、次のコマンドを実行して設定を変更します。

```
chown
cliqruser:cliqruser
/usr/local/osmosix/etc/gateway_config.properties
chmod 644 /usr/local/osmosix/etc/gateway_config.properties
```

h. 各サーバで次のコマンドを発行することによって、セカンダリ CCO とターシャリ CCO サーバで Tomcat を起動します。

```
/etc/init.d/tomcat start
```

i. HA モードのその他の CCO についてこの手順を繰り返し、CCM とその他の CCO 間の相互信頼を確立します。

CCO VM を登録し、設定が完了しました。ここでは、2 つのオプションがあります。

- その他のクラウド リージョンを追加し、これらのクラウドごとに CCO を登録します。詳細については、「クラウド リージョンごと(必須)」を参照してください。
- イメージをマッピングします。詳細については、「イメージ マッピング」を参照してください。

> クラウド アカウントのイメージを起動するアクセス許可を付与する必要がある場合は、「Image Launch Permissions」を参照してください。

- アプリケーションのモデリング、展開、および管理を行います。詳細については、「Application Profile」を参照してください。

戻る:クラウドの設定

- Dimension Data クラウドの設定

Dimension Data クラウドの設定

前提条件

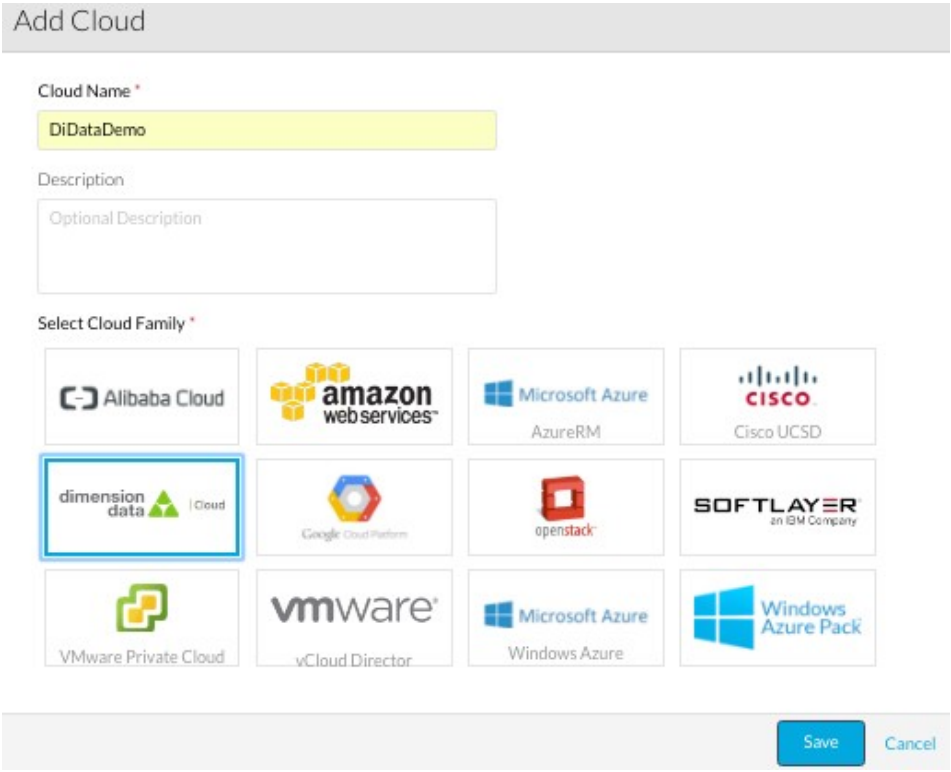
CloudCenter プラットフォームで Dimension Data クラウドをマッピングする前に、次の要件を確認します。

- VM を起動できる有効な Dimension Data CloudControl アカウント。
- 1 つ以上のネットワークドメインが目的のデータセンター内に作成されていて、ネットワークドメイン下に少なくとも 1 つの VLAN が作成されている。
- ネットワーク ドメインに少なくとも 1 つのパブリック IPv4 アドレス ブロックが追加されていて、ワーカー VM にパブリック IP を割り当てるために IP アドレスを使用できる。

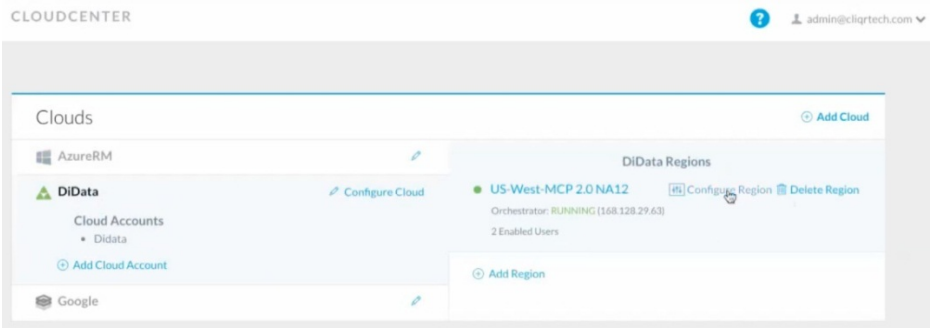
Dimension Data クラウドの設定

Dimension Data クラウドで論理マッピングを設定するには、次のプロセスに従います。

1. CCM UI にアクセスし、CCM UI のメインメニューで [管理(Admin)] > [クラウド(Clouds)] > [クラウドの追加(Add Cloud)] を選択します。



2. [Dimension Data] オプションを選択し、このクラウドの名前と説明を入力して、[保存(Save)] をクリックします。
3. 新たに追加されたクラウドを見つけて [クラウド アカウントの追加(Add Cloud Account)] をクリックし、このクラウド ファミリにアカウントを追加します。



[クラウド アカウントの追加(Add Cloud Account)] ポップアップが表示されます。

a. クラウド アカウントに**名前**を割り当てます。
b. Dimension Data クラウドのログイン クレデンシャルを入力します。
   i. Opsource(Dimension Data)アカウント名:Dimension Data クラウド アカウントのユーザ名。
   ii. パスワード:Dimension Data アカウントのパスワード。
c. [保存(Save)] をクリックします。新たに追加されたクラウドは [クラウド設定(Cloud Configurations)] ページに表示されます。

4. [リージョン(Region)] タブをクリックし、クラウド リージョンを追加します。
   a. [クラウド リージョンの追加(Add Cloud Region)] をクリックします。
   b. このクラウドに必要なリージョンを選択します。
   c. このクラウド リージョンの [リージョン名(Region Name)] およびオプションの [表示名(Display Name)] を追加します。
   d. [保存(Save)] をクリックします。

> インスタンス タイプ、ストレージ タイプ、およびイメージ マップのセクションは、リージョンを追加するとすぐに自動的に設定されます。

5. (任意)[クラウド設定の編集(Edit Cloud Settings)] をクリックし、[インスタンスの命名方法(Instance Naming Strategy)]、[インスタンス IPAM の使用(Instance IPAM Strategy)]、または [ノード名設定(Node Name Config)] フィールドを更新します。「VM Name Config」セクションでは、これらの値の設定の詳細を説明しています。

> **注意**
> **クラウド設定を編集**する場合、変更を CCO に保存し、これらの変更がファイアウォールの設定内の CCO にも反映されるようにする必要があります。
>
> CCO がすでに設定されている場合は、これらのクラウド設定を有効にするために CCO を再登録する必要があります。

6. クラウド設定を完了するには、CCO を CCM に登録する必要があります。
   CCM への CCO の登録

CCM への CCO の登録

- クラウド リージョンの微妙な違い
- 非 HA モード
- HA モード

クラウド リージョンの微妙な違い

CCM に CCO を登録すると、CCO は登録されたクラウド リージョンにのみ動作します。

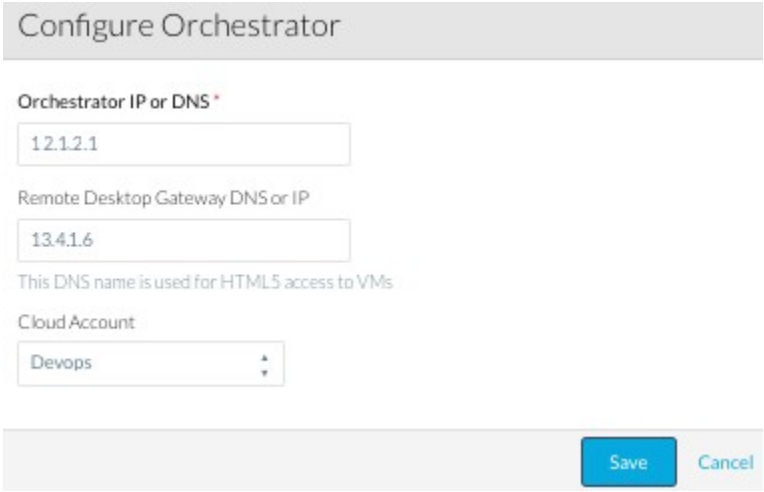
> **CloudCenter**
> CCM に CCO を登録すると、CloudCenter プラットフォームは、このクラウド リージョンがアクティブであると見なし、特定条件下でしか CloudCenter プラットフォームからこのクラウド リージョンを削除できなくなります。詳細については、「Cloud Region Configuration」>「*Delete Cloud Region*」を参照してください。

> 提供された例では AWS クラウドを参照していますが、スクリーン キャプチャはクラウドごとに異なることがある点に注意してください。

非 HA モード

CCM に CCO を登録するには、次の手順に従います。

a. [オーケストレータの設定（Configure Orchestrator）] ポップアップで、CCM からアクセス可能な CCO の IP アドレスを入力し、CCO をホストするために使用されるクラウド アカウントを選択します。



b. このページがまだ表示されていない場合は、必要なクラウドにおいて、[管理（Admin）] > [クラウド（Clouds）] > [リージョンの設定（Configure Regions）] を選択していることを確認します。
   i. [リージョン（Regions）] タブの [オーケストレータの設定（Configure Orchestrator）] をクリックします。
   ii. オーケストレータの IP または DNS（Orchestrator IP or DNS）：CCO サーバの IP または DNS アドレスを指定します。
   iii. リモート デスクトップ ゲートウェイの DNS または IP（Remote Desktop Gateway DNS or IP）：Guacamole サーバの IP アドレス（VM へのブラウザベースのアクセスを有効化）。Guacamole コンポーネントが AMQP サーバ内に存在している場合は、AMQP サーバの IP アドレスを指定します。
   iv. クラウド アカウント（Cloud Account）：この CCO で使用するクラウド アカウントを選択します。

> **Amazon クラウドの微妙な違い**
> IAM ロールを設定している場合、この設定は重要です。必ずこのロールを含むクラウド アカウントを選択してください。

c. [保存（Save）] をクリックします。これで、CCM と CCO の相互信頼関係が確立されました。CloudCenter プラットフォームは現在、導入された CCO によりクラウド リージョンを管理しています。
d. 手順 2 と手順 3 を繰り返し、CCM とその他の CCO 間の相互信頼を確立します。

CCO VM を登録し、設定が完了しました。ここでは、2 つのオプションがあります。

- その他のクラウド リージョンを追加し、これらのクラウドごとに CCO を登録します。詳細については、「クラウド リージョンごと（必須）」を参照してください。
- イメージをマッピングします。詳細については、「イメージ マッピング」を参照してください。

> クラウド アカウントのイメージを起動するアクセス許可を付与する必要がある場合は、「Image Launch Permissions」を参照してください。

- アプリケーションのモデリング、展開、および管理を行います。詳細については、「Application Profile」を参照してください。

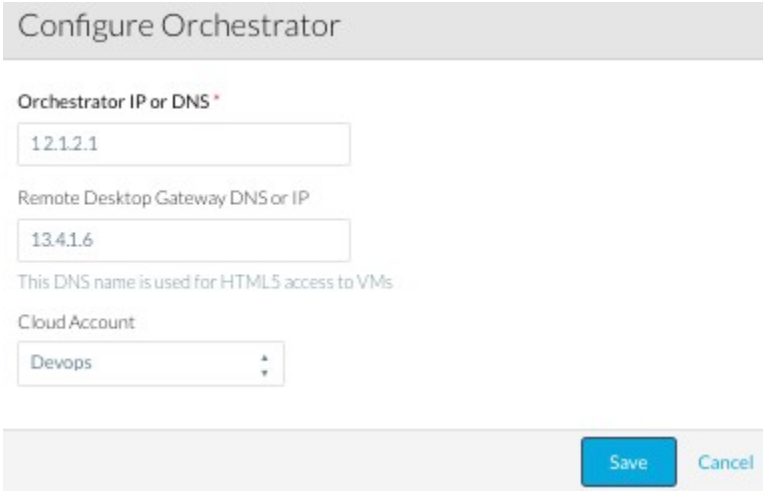
HA モード

CCM に CCO を登録するには、次の手順に従います。

a. プライマリ CCO で Tomcat Service が実行中であることを確認します。
b. セカンダリ CCO およびターシャリ CCO にログインし、両方のサーバで Tomcat Service を停止します。

```
/etc/init.d/tomcat stop
```

c. CCM UI にアクセスし、CCO LB の IP アドレスを使用して CCO を登録します。
   i. このページがまだ表示されていない場合は、必要なクラウドにおいて、[管理（Admin）] > [クラウド（Clouds）] > [リージョンの設定（Configure Regions）] を選択していることを確認します。
   ii. [リージョン（Regions）] タブの [オーケストレータの設定（Configure Orchestrator）] をクリックします。
   iii. CCM からアクセス可能な CCO の IP アドレスを入力し、CCO をホストするために使用されるクラウド アカウントを選択します。



      1. オーケストレータの IP または DNS（Orchestrator IP or DNS）：CCO サーバの IP または DNS アドレスを指定します。
      2. リモート デスクトップ ゲートウェイの DNS または IP（Remote Desktop Gateway DNS or IP）：Guacamole サーバの IP アドレス（VM へのブラウザベースのアクセスを有効化）。Guacamole コンポーネントが AMQP サーバ内に存在している場合は、AMQP サーバの IP アドレスを指定します。
      3. クラウド アカウント（Cloud Account）：この CCO で使用するクラウド アカウントを選択します。必ずこのロールを含むクラウド アカウントを選択してください。
      4. [保存（Save）] をクリックします。これで、CCM と CCO の相互信頼関係が確立されました。CloudCenter プラットフォームは現在、導入された CCO によりクラウド リージョンを管理しています。
d. 登録が成功したら、プライマリ CCO サーバにログインします。
e. プライマリ CCO の **/usr/local/osmosix/etc/** フォルダから、セカンダリ CCO およびターシャリ CCO の両サーバ上の**同じ場所**に **gateway_config.properties** ファイルをコピーします。
f. すべてのサーバのコピーしたファイルの所有権およびアクセス許可が次のようになっていることを確認します。
   - オーナー（Owner）= cliqruser
   - グループ権限（Group Permission）= 読み取りおよび書き込み
g. 必要な場合は、次のコマンドを実行して設定を変更します。

```
chown
cliqruser:cliqruser
/usr/local/osmosix/etc/gateway_config.properties
chmod 644 /usr/local/osmosix/etc/gateway_config.properties
```

h. 各サーバで次のコマンドを発行することによって、セカンダリ CCO とターシャリ CCO サーバで Tomcat を起動します。

```
/etc/init.d/tomcat start
```

i. HA モードのその他の CCO についてこの手順を繰り返し、CCM とその他の CCO 間の相互信頼を確立します。

CCO VM を登録し、設定が完了しました。ここでは、2 つのオプションがあります。

- その他のクラウド リージョンを追加し、これらのクラウドごとに CCO を登録します。詳細については、「クラウド リージョンごと(必須)」を参照してください。
- イメージをマッピングします。詳細については、「イメージ マッピング」を参照してください。

> クラウド アカウントのイメージを起動するアクセス許可を付与する必要がある場合は、「Image Launch Permissions」を参照してください。

- アプリケーションのモデリング、展開、および管理を行います。詳細については、「Application Profile」を参照してください。

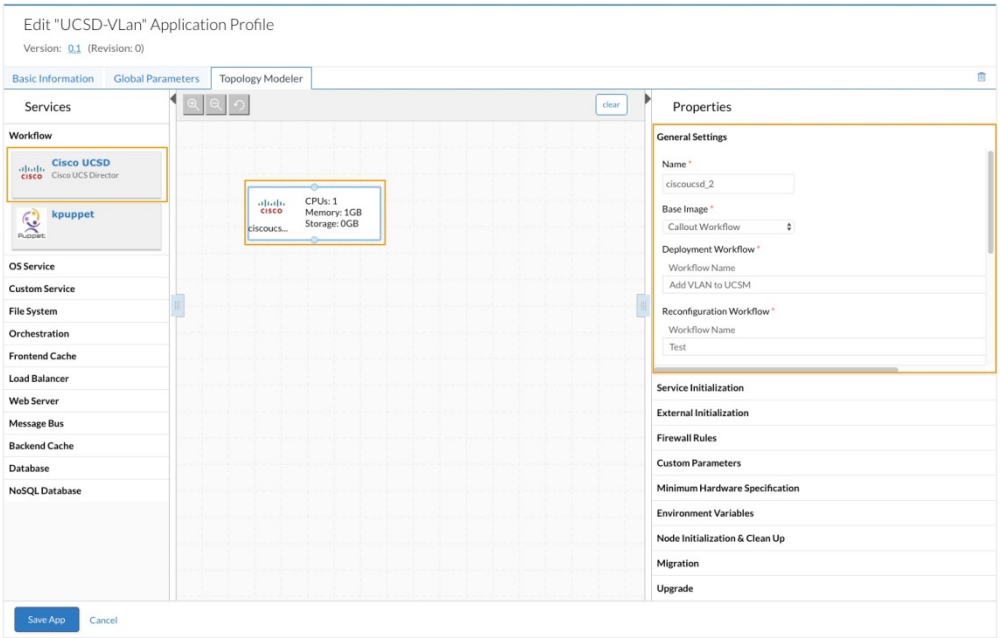
戻る:クラウドの設定

- Cisco UCSD クラウドの設定

Cisco UCSD クラウドの設定

CloudCenter プラットフォームは、ユニファイド コンピューティング システム ディレクタ(UCSD)コールアウトのワークフローを呼び出せるようにする Cisco UCSD の統合を実装します。ユーザは Cisco UCSD サービスを CloudCenter のトポロジ モデラーにドラッグ アンド ドロップし、1 つまたは複数の UCSD コールアウトを使用してトポロジを作成できます。これにより、企業は UCSD コールアウトを使用するアプリケーションの混在トポロジを作成することができ、次の利点を得ることができます。

- 企業はガバナンスとワークフロー管理に CloudCenter を使用できる。
- システム管理者は UCSD を使用して物理ストレージをプロビジョニングできる。



制限事項

この統合を使用する場合は、次の制限事項に注意してください。

- リリースの互換性の詳細については、「フェーズ 1：インフラストラクチャの準備」を参照してください。
- USCD のこの統合の実装により、ネットワーク アプライアンスのストレージ設定をプロビジョニングできるようになる（CloudCenter プラットフォームについてテストおよび確認済み）。

> ⚠ 現在、UCSD では VM をプロビジョニングできます。

- この機能は、限定されたお客様に対してテストおよび実装されている。
- このバージョンでは、このページで明示的に説明した統合のみがサポートされている。
- この統合には Worker1 のアプライアンスは必要ない。
- この統合では、CCM アプライアンスおよび CCO アプライアンスは使用できない。
- クラウド リージョンに対して*外部初期化スクリプト*（「External Service」を参照）を作成し、CCM から UCSD ワークフローを起動するとき、ワークフローは実行されますが、リージョンレベルの*外部初期化スクリプト*は実行されません。これは、*外部初期化スクリプト*（PreVM init）は一般的に VM の起動前に実行され、UCSD で起動されている VM がないためです。

統合要件

Cisco UCSD と統合するには、CloudCenter のシステム管理者は次の条件を順守する必要があります。

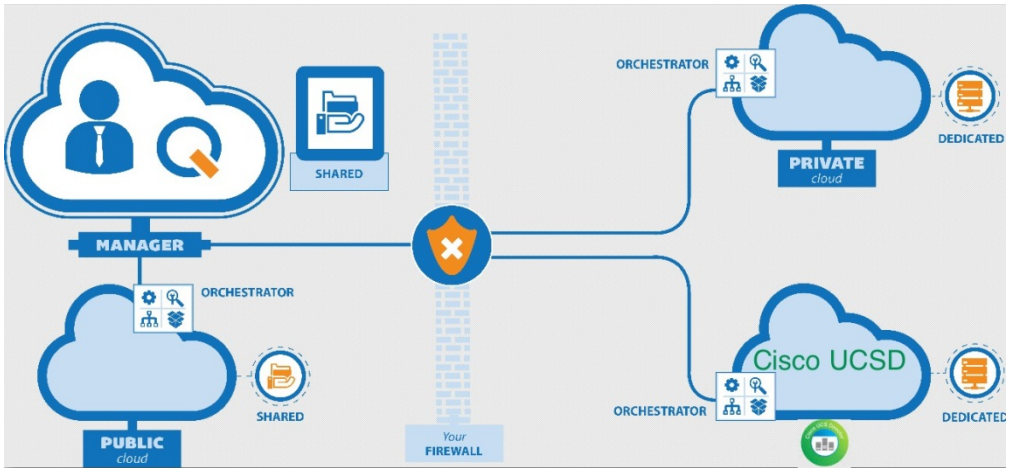
- Cisco UCSD アカウントと環境にアクセスする管理者機能。

> ⚠ 企業内で UCSD を統合する場合は、エンドツーエンドの導入を実行するための UCSD 環境に対するアクセス権が CloudCenter プラットフォームに必要です。

- CloudCenter プラットフォームによって呼び出される UCSD のワークフローのリストに関する知識。

> ✓ CloudCenter プラットフォームでは、UCSD が公開するコールアウト フローを使用するため、オーケストレーション プロセスを抽象化します。CloudCenter プラットフォームは、クラウドのガバナンスと管理を目的としてのみ、公開された UCSD パラメータを使用します。

- Cisco UCSD の各インスタンスは、アプリケーションをモデル化する前に、CCO と関連付ける必要がある。



- 現時点では、1 つの CloudCenter で 1 つの UCSD インスタンスをサポートする。
- CloudCenter の UCSD の各実装には、関連付けられた物理イメージのエントリが CloudCenter プラットフォーム内に必要です（このエントリは、論理イメージが使用されない場合でも、ダミーのプレースホルダとなります）。

UCSD ワークフローのサポート

UCSD には、ワークフローの概念があります。これらのワークフローは、企業や導入環境により異なります。一例として、UCSD の統合を使用してストレージをプロビジョニングする場合のワークフローでは、CloudCenter は現在、次のワークフローを呼び出します。

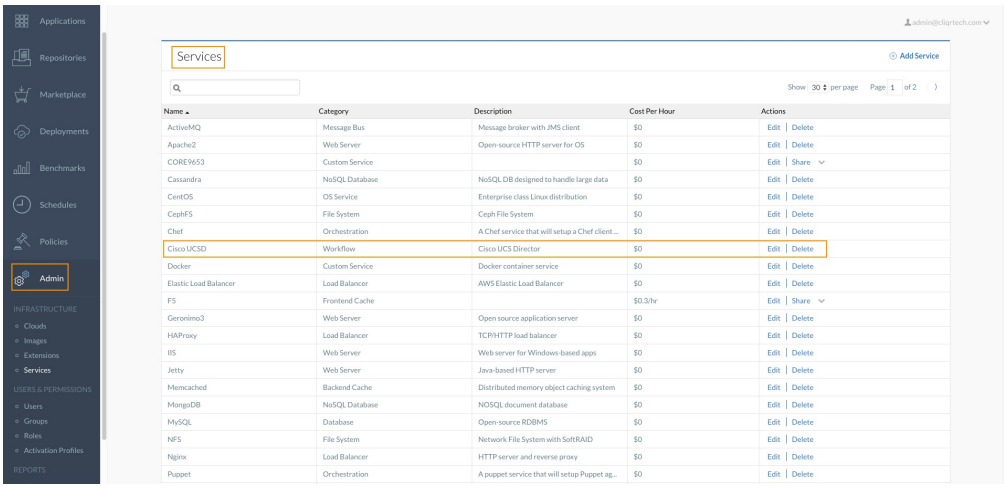
- 新しい記憶域の作成
- 記憶域の存在の検証
- 既存の記憶域の更新
- 記憶域の削除
- 記憶域に関する情報の取得

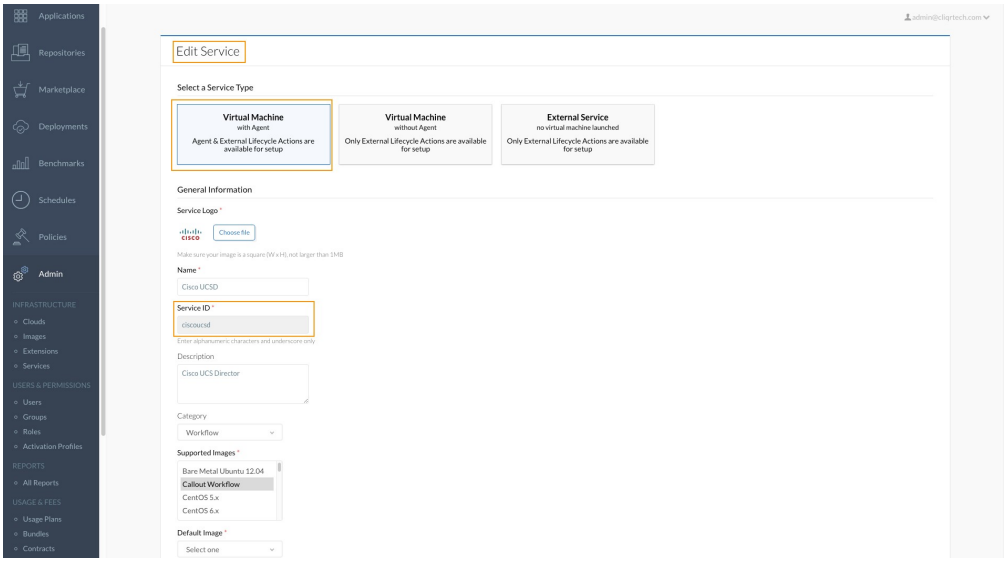
カスタム サービスとしての UCSD の設定

現在の UCSD のワークフローは、企業の追加のストレージ作業域の作成とメンテナンスに固有のものです。UCSD が 1 つの CCO に関連付けられているため、記憶域に関する情報にアクセスするたびに、CCO は許可された UCSD ワークフローを取得します。

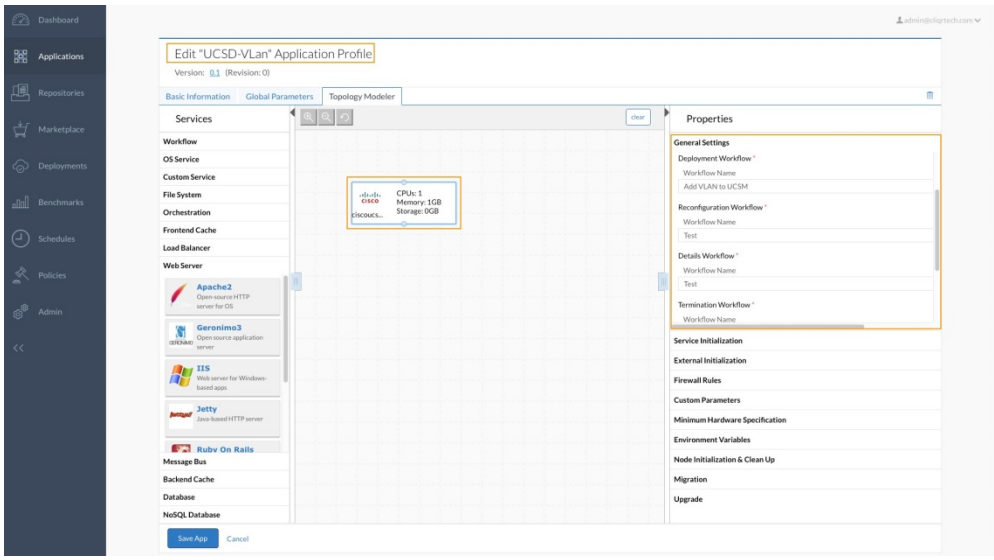
UCSD をカスタム サービスとして設定、定義、使用するには、次のプロセスを実行します。

1. CCM UI にアクセスし、CCM UI のメインメニューで [管理(Admin)] > [クラウド(Clouds)] > [クラウドの追加(Add Cloud)] を選択します。
   - クラウド タイプ(Cloud Type) : **UCSD**
   - クラウド ファミリ(Cloud Family) : **Cisco UCSD**
   - リージョン(Region) : ユーザ設定が可能な名前
2. ダミーの UCSD 物理イメージを設定し(「イメージ ID の設定」を参照)、このイメージをマッピングします。
3. **Cisco UCSD** サービスを編集し、許可された UCSD ワークフロー パラメータを定義します。「Custom Service Definition」を参照してください。

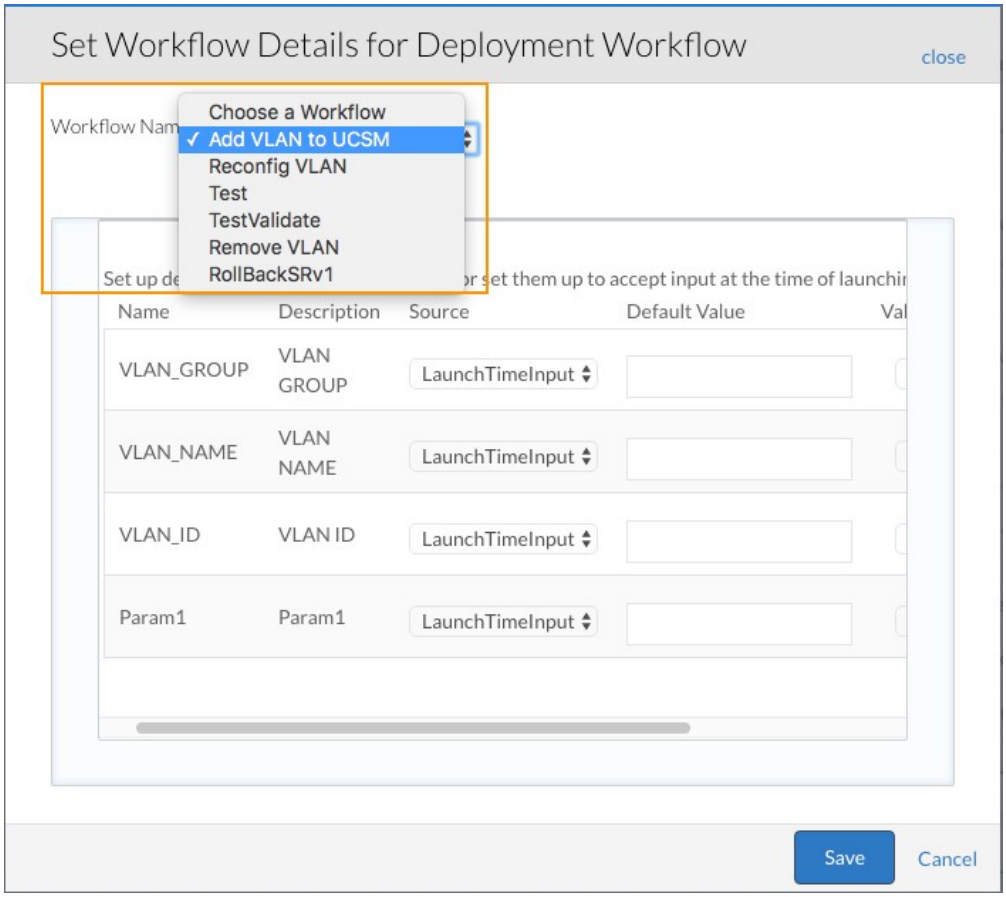




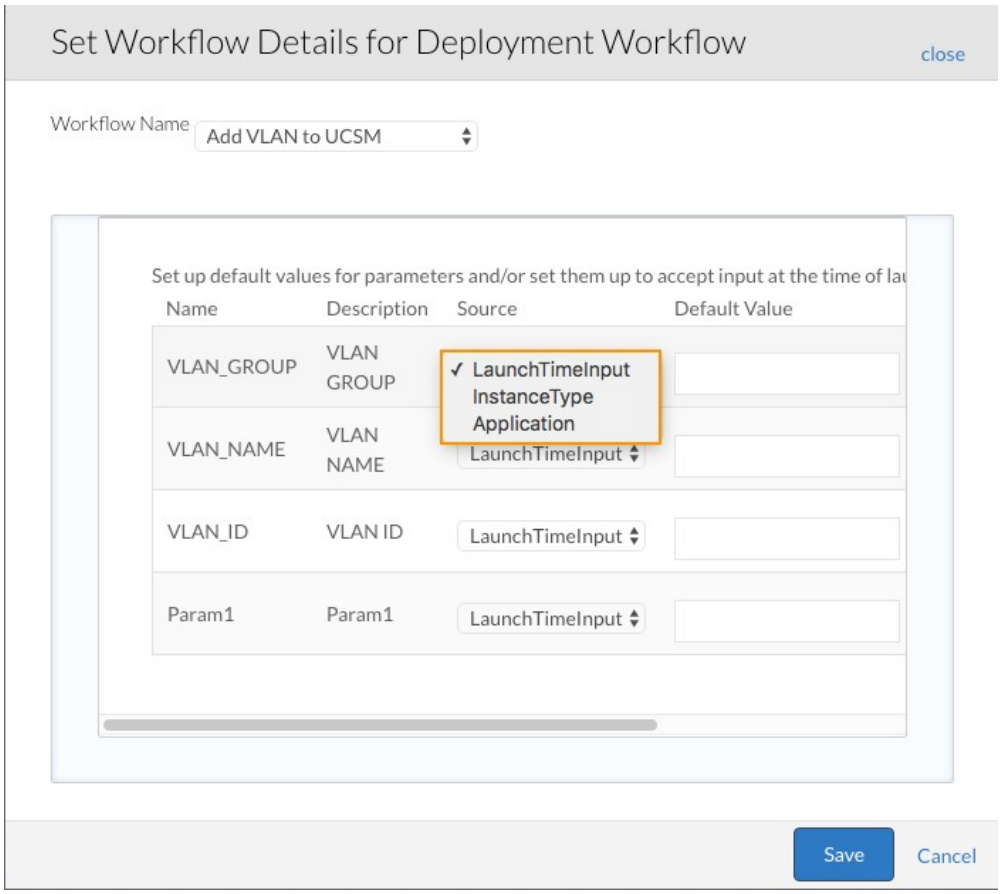
4. アプリケーションをモデル化し、UCSD サービスを使用します。UCSD サービスを選択すると、定義した UCSD サービスのパラメータが [トポロジ モデラー(Topology Modeler)] の [*サービス(Services)*] ページの [カスタム サービス(Custom Service)] セクション(右側のペイン)に表示されます。



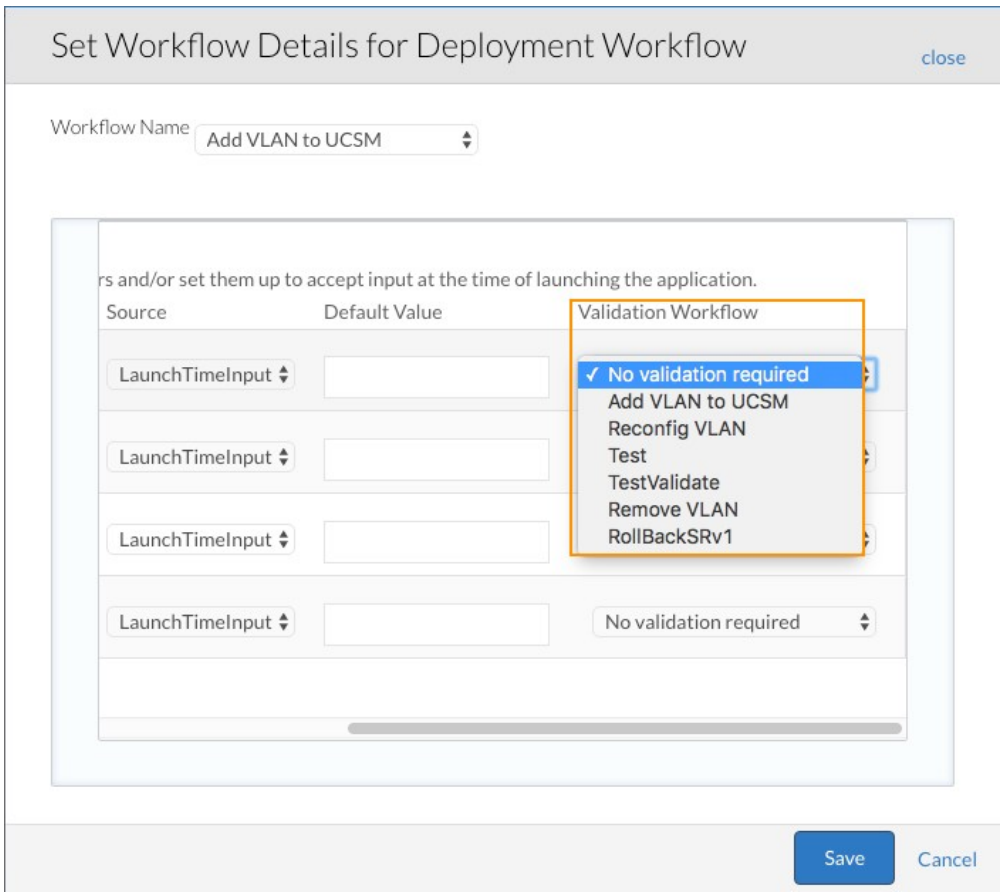
5. 必要に応じて、追加のグローバル パラメータを追加できます。「Topology Modeler」>「*Global Parameters*」を参照してください。
6. 設定済みの UCSD のワークフローのリストが [一般設定(General Settings)] セクションに表示されます。設定済みのワークフローをクリックすると、その特定のワークフローに関連付けられているパラメータが表示されます。



7. ドロップダウン リストからこのワークフローの各パラメータのソースを選択します。
   - LaunchTimeinput:ユーザによるアプリケーション導入時に、このパラメータをオーバーライドできることを示します。
   - InstanceType:アプリケーション導入時にインスタンス タイプを選択すると、そのインスタンス タイプに関連付けられているストレージ サイズがこのパラメータの値になります。
   - Application:導入時に使用されるデフォルト値を入力します(オーバーライドできません)。



8. 該当する場合は、ドロップダウン リストから必要な [検証ワークフロー（Validation Workflow）] をパラメータごとに選択することもできます。このリストは、導入ごとに固有のものであり、該当するワークフローのみを表示するようにフィルタリングすることもできます。



9. UCSD アプリケーションを起動します。

これで、UCSD をカスタム サービスとして設定し、起動しています。

戻る:クラウドの設定

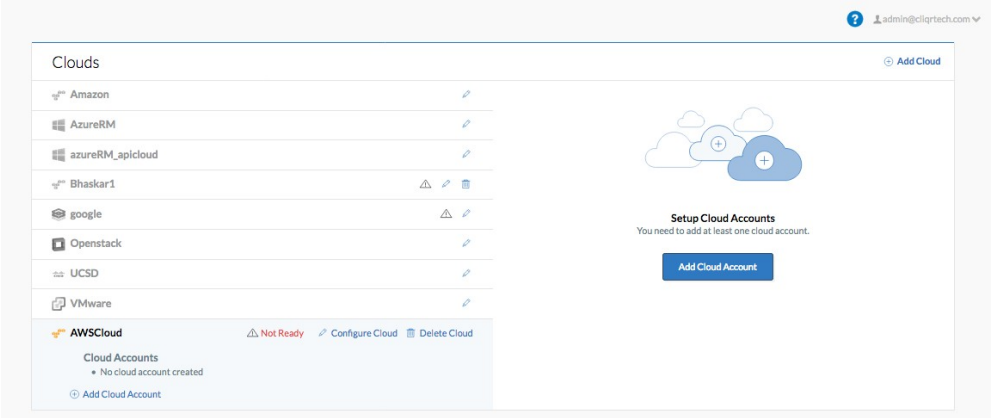
- AWS クラウドの設定

Amazon クラウドの設定

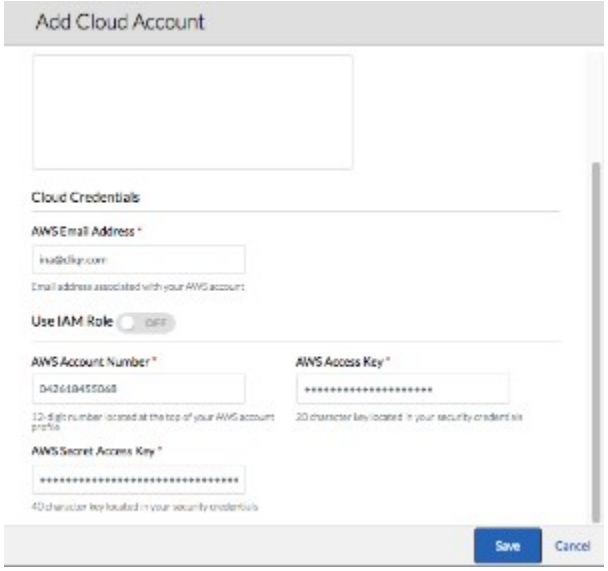
Amazon Web Services(AWS)クラウドで論理マッピングを設定するには、次のプロセスに従います。

1. CCM UI にアクセスし、CCM UI のメインメニューで [管理(Admin)] > [クラウド(Clouds)] > [クラウドの追加(Add Cloud)] を選択します。

2. [Amazon Web Services] オプションを選択し、このクラウドの名前と説明を入力して、[保存(Save)] をクリックします。
3. 新たに追加されたクラウドを見つけて [クラウド アカウントの追加(Add Cloud Account)] をクリックし、このクラウド ファミリにアカウントを追加します。



[クラウド アカウントの追加(Add Cloud Account)] ポップアップが表示されます。



1. a. クラウド アカウントに**名前**を割り当てます。
   b. AWS クラウド クレデンシャルを入力します。
      i. AWS 電子メールアドレス（AWS Email Address）：AWS クラウド ファミリのアカウントに関連付けられている電子メールアドレス。
      ii. IAM ロールを使用（Use IAM Role）：

IAM ロール

Identity and Access Management（IAM）ロールとセキュリティ トークン サービス（STS）は、CloudCenter プラットフォームによりサポートされています。

> **機能の依存性**
> これらの 2 つの機能は、IAM ロールを使用して**起動する CCO**（および AWS での信頼関係の確立）に依存しています。詳細については、http://docs.aws.amazon.com を参照してください。

> IAM ロールを使用するには、管理者ロールで CCO VM を起動する必要があります。こうすると IAM ロールをそれ以降いつでも使用できます。管理者ロールで CCO VM を起動すると、IAM ロールまたはクラシック キー/秘密キーによるアクセスのいずれかをいつでも使用できるようになります。
>
> IAM ロールベースのアカウントの場合、CloudCenter プラットフォームは *EC2fullAccess* ロールが必要です（最小要件）。CloudCenter RDS の設定済みサービスを使用する場合、アカウントにはさらに *RDSfullAccess* も必要です。

アクセス キーや秘密キーなどを指定する代わりに、IAM ロールを使用してインスタンス タイプを管理できます。デフォルトでは、この機能は無効になっています。AWS クラウドを設定するときは、このボタンを **ON** に切り替えることで IAM ロールを明示的に有効にする必要があります。

> 次の要件を満たしている場合、IAM ロール ベースのアカウントを使用して、RDS インスタンスを起動できます。
>
> - Docker コンテナが CCO の一部でない場合は、Docker コンテナ VM を CCO サーバと同じ IAM ロールに割り当てる必要があります。
> - 次の *sts:GetFederationToken* カスタム ポリシーを、（RDSfullAccess とともに）IAM ロールに接続していることを確認します。

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Action": "sts:GetFederationToken",
        "Resource": "*"
    }]
}
```

iii. AWS アカウント番号（AWS Account Number）：AWS アカウントのアカウント番号。
iv. AWS アクセス キーと秘密キー：この AWS アカウントにアクセスするためのセキュリティ クレデンシャル。

c. [保存（Save）] をクリックします。新たに追加されたクラウドは [クラウド設定（Cloud Configurations）] ページに表示されます。

2. [リージョン（Region）] タブをクリックし、クラウド リージョンを追加します。
   a. [クラウド リージョンの追加（Add Cloud Region）] をクリックします。
   b. このクラウドに必要なリージョンを選択します。
   c. このクラウド リージョンの [リージョン名（Region Name）] およびオプションの [表示名（Display Name）] を追加します。
   d. [保存（Save）] をクリックします。

> インスタンス タイプ、ストレージ タイプ、およびイメージ マップのセクションは、リージョンを追加するとすぐに自動的に設定されます。

3. （任意）[クラウド設定の編集（Edit Cloud Settings）] をクリックし、[インスタンスの命名方法（Instance Naming Strategy）]、[インスタンス IPAM の使用（Instance IPAM Strategy）]、または [ノード名設定（Node Name Config）] フィールドを更新します。「VM Name Config」セクションでは、これらの値の設定の詳細を説明しています。

> **注意**
> **クラウド設定を編集**する場合、変更を CCO に保存し、これらの変更がファイアウォールの設定内の CCO にも反映されるようにする必要があります。
>
> CCO がすでに設定されている場合は、これらのクラウド設定を有効にするために CCO を再登録する必要があります。

4. クラウド設定を完了するには、CCO を CCM に登録する必要があります。
   CCM への CCO の登録

CCM への CCO の登録

- クラウド リージョンの微妙な違い
- 非 HA モード
- HA モード

クラウド リージョンの微妙な違い

CCM に CCO を登録すると、CCO は登録されたクラウド リージョンにのみ動作します。

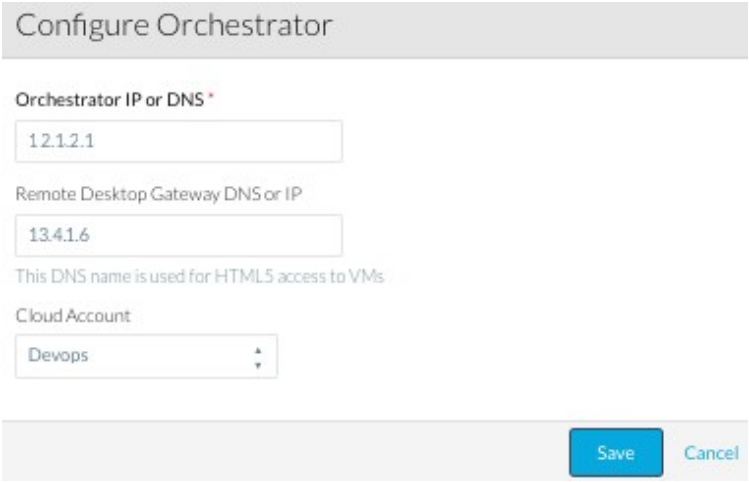
> **CloudCenter**
> CCM に CCO を登録すると、CloudCenter プラットフォームは、このクラウド リージョンがアクティブであると見なし、特定条件下でしか CloudCenter プラットフォームからこのクラウド リージョンを削除できなくなります。詳細については、「Cloud Region Configuration」>「*Delete Cloud Region*」を参照してください。

> 提供された例では AWS クラウドを参照していますが、スクリーン キャプチャはクラウドごとに異なることがある点に注意してください。

非 HA モード

CCM に CCO を登録するには、次の手順に従います。

a. [オーケストレータの設定（Configure Orchestrator）] ポップアップで、CCM からアクセス可能な CCO の IP アドレスを入力し、CCO をホストするために使用されるクラウド アカウントを選択します。



b. このページがまだ表示されていない場合は、必要なクラウドにおいて、[管理（Admin）] > [クラウド（Clouds）] > [リージョンの設定（Configure Regions）] を選択していることを確認します。
   i. [リージョン（Regions）] タブの [オーケストレータの設定（Configure Orchestrator）] をクリックします。
   ii. オーケストレータの IP または DNS（Orchestrator IP or DNS）：CCO サーバの IP または DNS アドレスを指定します。
   iii. リモート デスクトップ ゲートウェイの DNS または IP（Remote Desktop Gateway DNS or IP）：Guacamole サーバの IP アドレス（VM へのブラウザベースのアクセスを有効化）。Guacamole コンポーネントが AMQP サーバ内に存在している場合は、AMQP サーバの IP アドレスを指定します。
   iv. クラウド アカウント（Cloud Account）：この CCO で使用するクラウド アカウントを選択します。

> **Amazon クラウドの微妙な違い**
> IAM ロールを設定している場合、この設定は重要です。必ずこのロールを含むクラウド アカウントを選択してください。

c. [保存（Save）] をクリックします。これで、CCM と CCO の相互信頼関係が確立されました。CloudCenter プラットフォームは現在、導入された CCO によりクラウド リージョンを管理しています。
d. 手順 2 と手順 3 を繰り返し、CCM とその他の CCO 間の相互信頼を確立します。

CCO VM を登録し、設定が完了しました。ここでは、2 つのオプションがあります。

- その他のクラウド リージョンを追加し、これらのクラウドごとに CCO を登録します。詳細については、「クラウド リージョンごと（必須）」を参照してください。
- イメージをマッピングします。詳細については、「イメージ マッピング」を参照してください。

> クラウド アカウントのイメージを起動するアクセス許可を付与する必要がある場合は、「Image Launch Permissions」を参照してください。

- アプリケーションのモデリング、展開、および管理を行います。詳細については、「Application Profile」を参照してください。

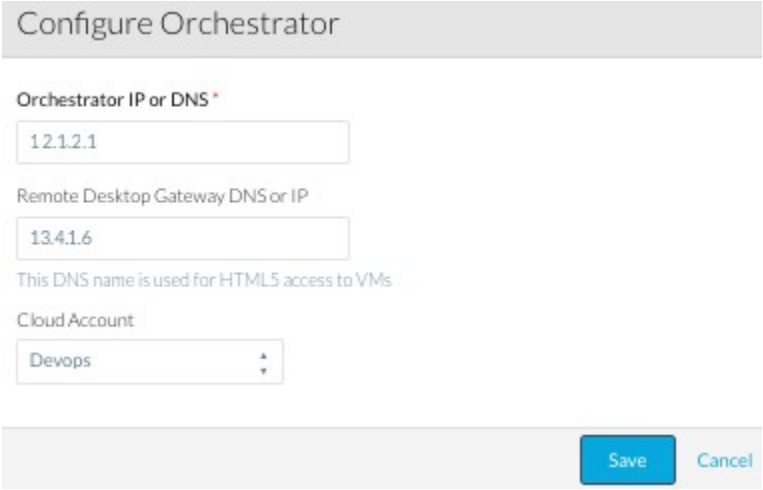
HA モード

CCM に CCO を登録するには、次の手順に従います。

a. プライマリ CCO で Tomcat Service が実行中であることを確認します。
b. セカンダリ CCO およびターシャリ CCO にログインし、両方のサーバで Tomcat Service を停止します。

```
/etc/init.d/tomcat stop
```

c. CCM UI にアクセスし、CCO LB の IP アドレスを使用して CCO を登録します。
   i. このページがまだ表示されていない場合は、必要なクラウドにおいて、[管理（Admin）] > [クラウド（Clouds）] > [リージョンの設定（Configure Regions）] を選択していることを確認します。
   ii. [リージョン（Regions）] タブの [オーケストレータの設定（Configure Orchestrator）] をクリックします。
   iii. CCM からアクセス可能な CCO の IP アドレスを入力し、CCO をホストするために使用されるクラウド アカウントを選択します。



1. オーケストレータの IP または DNS（Orchestrator IP or DNS）：CCO サーバの IP または DNS アドレスを指定します。
2. リモート デスクトップ ゲートウェイの DNS または IP（Remote Desktop Gateway DNS or IP）：Guacamole サーバの IP アドレス（VM へのブラウザベースのアクセスを有効化）。Guacamole コンポーネントが AMQP サーバ内に存在している場合は、AMQP サーバの IP アドレスを指定します。
3. クラウド アカウント（Cloud Account）：この CCO で使用するクラウド アカウントを選択します。必ずこのロールを含むクラウド アカウントを選択してください。
4. [保存（Save）] をクリックします。これで、CCM と CCO の相互信頼関係が確立されました。CloudCenter プラットフォームは現在、導入された CCO によりクラウド リージョンを管理しています。

d. 登録が成功したら、プライマリ CCO サーバにログインします。
e. プライマリ CCO の **/usr/local/osmosix/etc/** フォルダから、セカンダリ CCO およびターシャリ CCO の両サーバ上の**同じ場所**に **gateway_config.properties** ファイルをコピーします。
f. すべてのサーバのコピーしたファイルの所有権およびアクセス許可が次のようになっていることを確認します。
   - オーナー（Owner）= cliqruser
   - グループ権限（Group Permission）= 読み取りおよび書き込み
g. 必要な場合は、次のコマンドを実行して設定を変更します。

```
chown
cliqruser:cliqruser
/usr/local/osmosix/etc/gateway_config.properties
chmod 644 /usr/local/osmosix/etc/gateway_config.properties
```

h. 各サーバで次のコマンドを発行することによって、セカンダリ CCO とターシャリ CCO サーバで Tomcat を起動します。

```
/etc/init.d/tomcat start
```

i. HA モードのその他の CCO についてこの手順を繰り返し、CCM とその他の CCO 間の相互信頼を確立します。

CCO VM を登録し、設定が完了しました。ここでは、2 つのオプションがあります。

- その他のクラウド リージョンを追加し、これらのクラウドごとに CCO を登録します。詳細については、「クラウド リージョンごと（必須）」を参照してください。
- イメージをマッピングします。詳細については、「イメージ マッピング」を参照してください。

> クラウド アカウントのイメージを起動するアクセス許可を付与する必要がある場合は、「Image Launch Permissions」を参照してください。

- アプリケーションのモデリング、展開、および管理を行います。詳細については、「Application Profile」を参照してください。

戻る：クラウドの設定

- Azure RM クラウドの設定

Azure RM クラウドの設定

> 次のスクリーン キャプチャは、Azure ポータルが変更されると変わる可能性があることに注意してください。この項ではあくまでも参考として示しています。

前提条件

Azure Resource Manager クラウドをマッピングする前に、次の要件を確認してください。有効な

- Windows Azure Resource Manager アカウントを持っている。
- Azure CLI の ARM モードにログインし、必要な Azure プロバイダーを登録します。

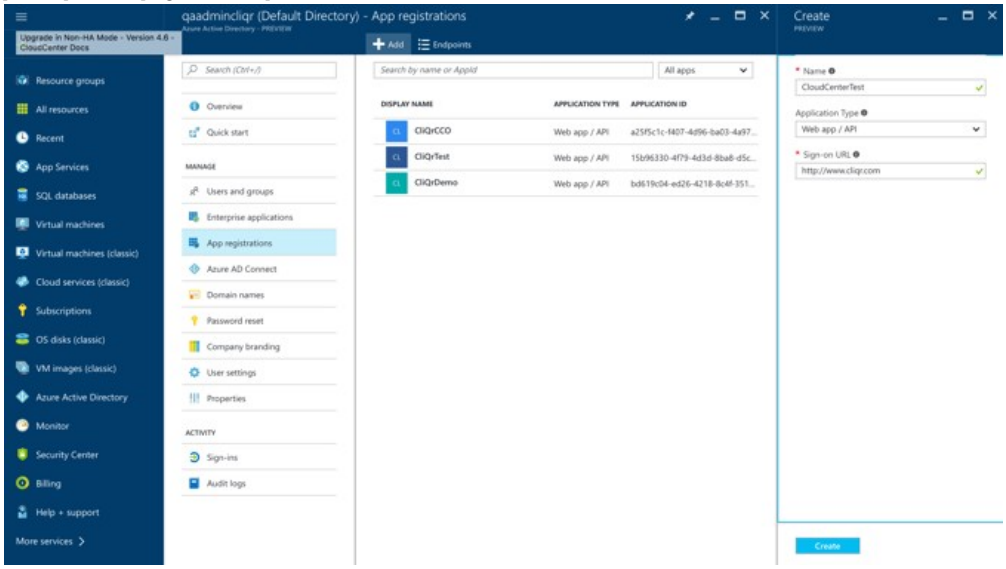
> この手順は、Azure CLI の使用によってのみ実行できます。

1. Azure CLI をプラットフォームにインストールします。詳細については、https://docs.microsoft.com/en-us/azure/cli-install-nodejs を参照してください。
2. Azure CLI にログインします。
   azure login
3. ARM モードを使用していることを確認します。
   azure config mode arm
4. Azure プロバイダーを登録します。
   azure provider register Microsoft.Compute Microsoft.Storage Microsoft.Network Microsoft.Resources Microsoft.Authorization

   > PowerShell を使用している場合、次のコマンドを発行します。
   > **Register-AzureProvider**

5. Azure プロバイダーが登録されていることを確認します。
   azure provider list

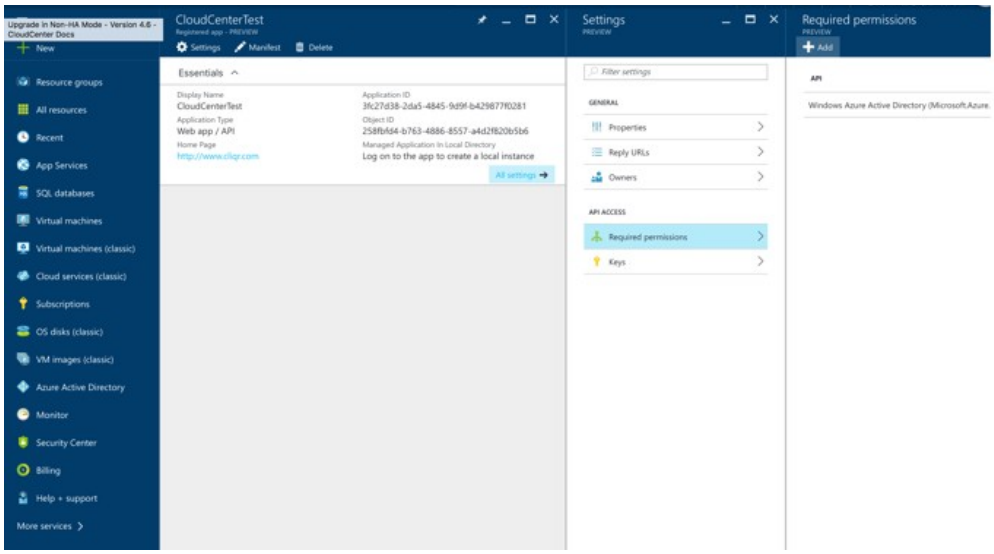
- [Azure Resource ManagerPortal] で、[Azure Active Directory] ページに移動します。
  a. [App Registration] を選択し、[Add] をクリックします。
  b. [Name] および [Sign on URL] に入力し、アプリケーションを**作成**します。



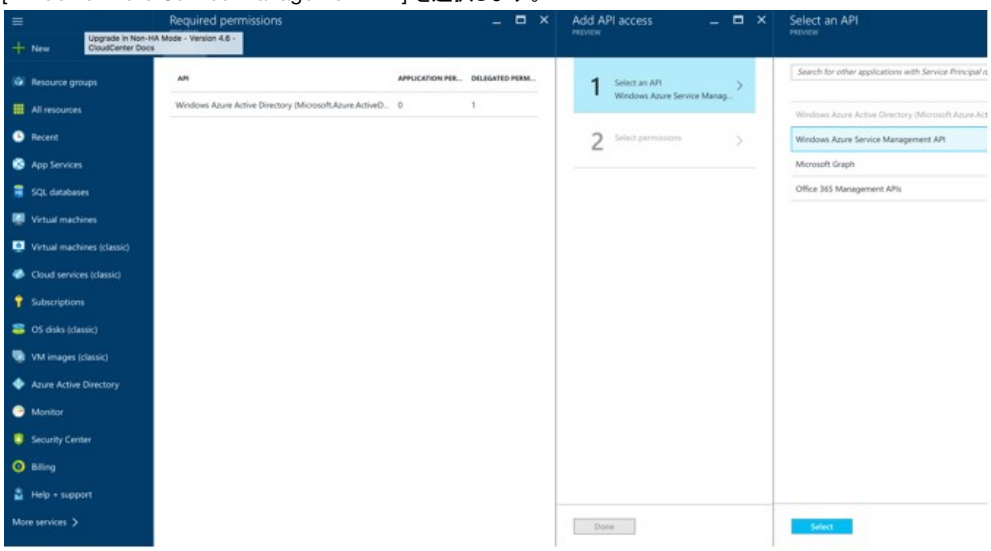
  c. 新しく作成されたアプリケーションを選択します。

> **アプリケーション ID を書き留めてください。CloudCenter でクラウド アカウントを作成するときに必要です(クライアント ID になります)。**

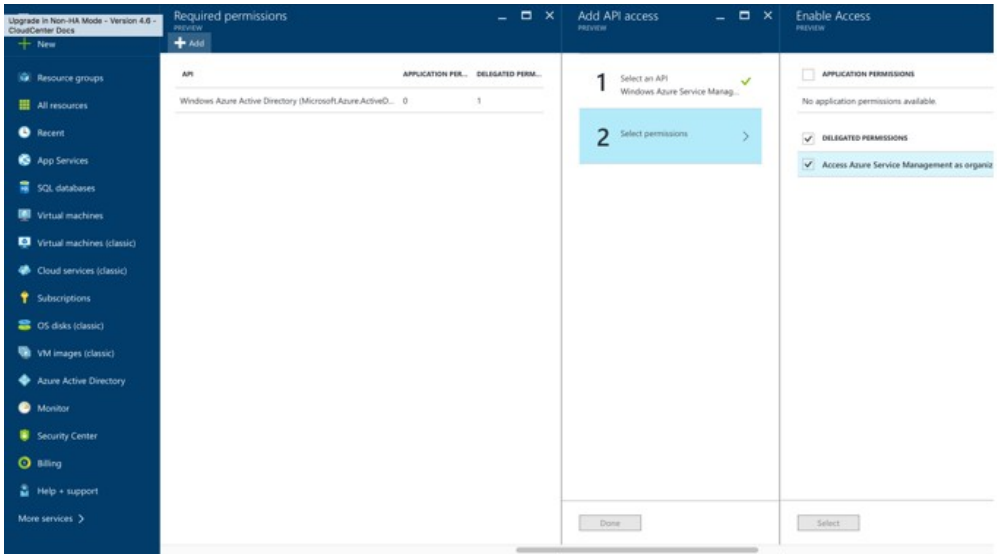
  d. [All Settings] をクリックします。
  e. [API Access] の下にある [Required Permission] を選択し、[Add] をクリックします。

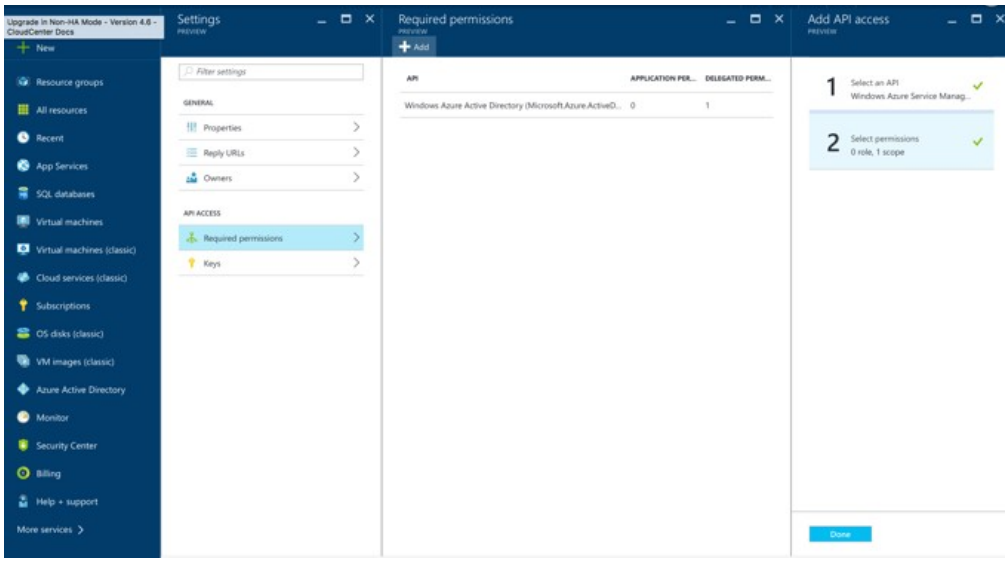


f. [Windows Azure Service Management API] を選択します。



g. 権限として [Delegated Permission] を選択し、[Done] をクリックします。

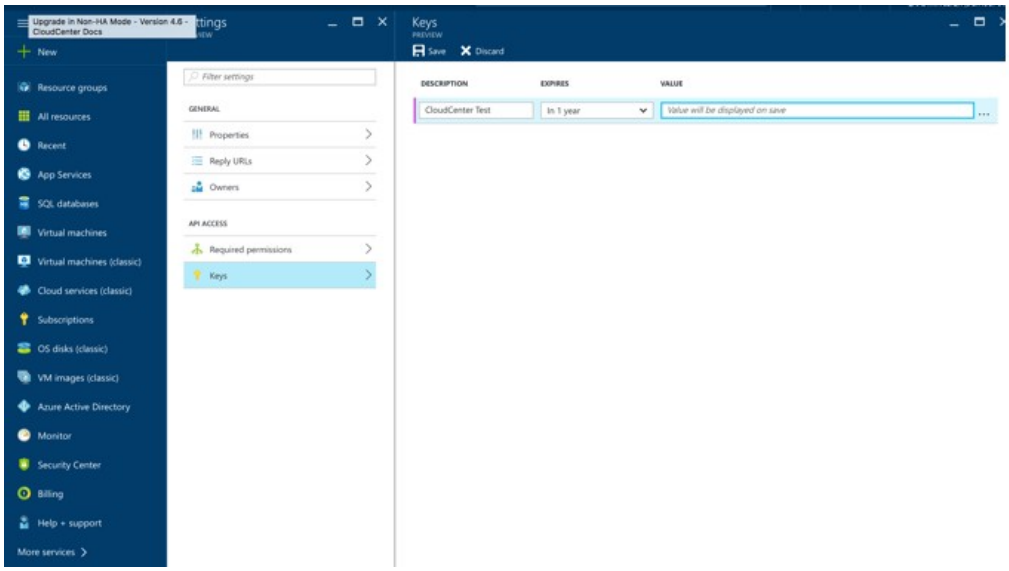




h. [API Access] の下にある [Keys] を選択します。

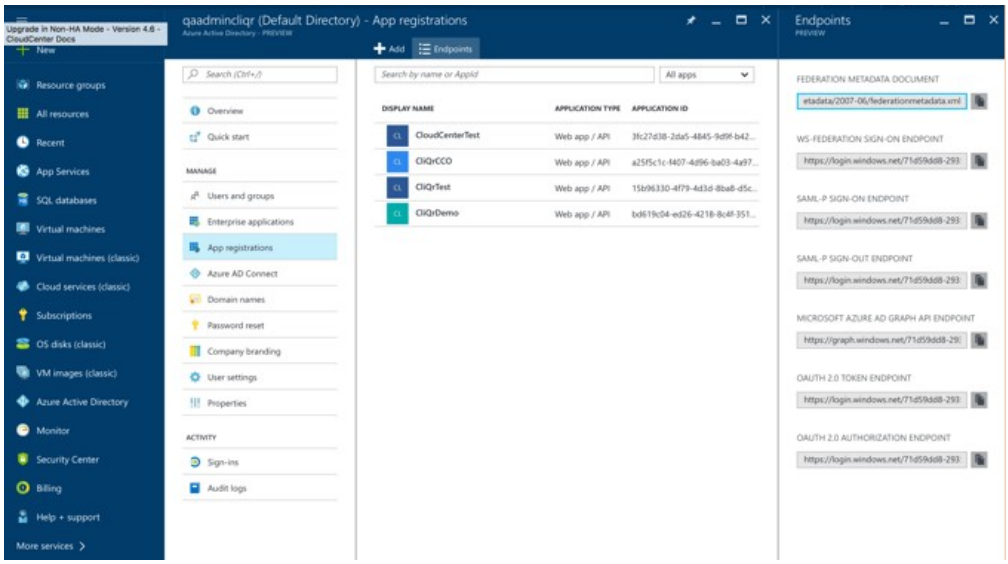
i. [Description]、[Expires] を指定し、[Save] クリックします。

> **[Save] をクリックした後、キーを書き留めてください。このキーを後でポータルから取得することはできません。このキーは、クラウド アカウントを作成する際に、クライアント キーとして CloudCenter ポータルで使用されます。**

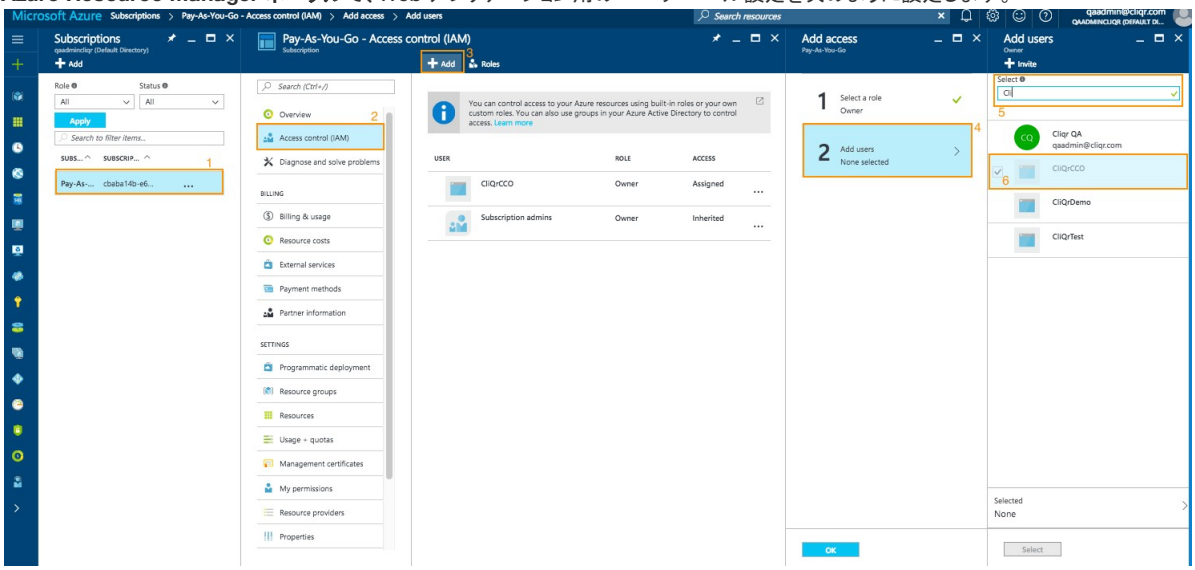


j. [App Registration] を選択し、[Endpoints] をクリックします。

> **[OAuth 2.0 Authorization Endpoint] のテナント ID を書き留めてください。この ID は、クラウド アカウントを作成する際に、CloudCenter ポータルで使用されます。**



- **Azure Resource Manager ポータル**で、Web アプリケーション用のユーザ ロール設定を次のように設定します。



1. [Subscription] > [Valid subscription]（これは管理するサブスクリプションです）を選択します。
2. [Access control (IAM)] をクリックします。
3. [managed subscription] ペインの右上隅にある [+Add] アイコンをクリックします。
4. [Add User] をクリックし、[OWNER] ロールを選択します。より詳細な管理をするために、他のロールを選択することもできます。

> このロールは、ストレージ、コンピューティング、ネットワーク、keyvault などの Azure RM リソースにアクセスして管理でき、CloudCenter プラットフォーム用の AzureRM を設定できる必要があります。

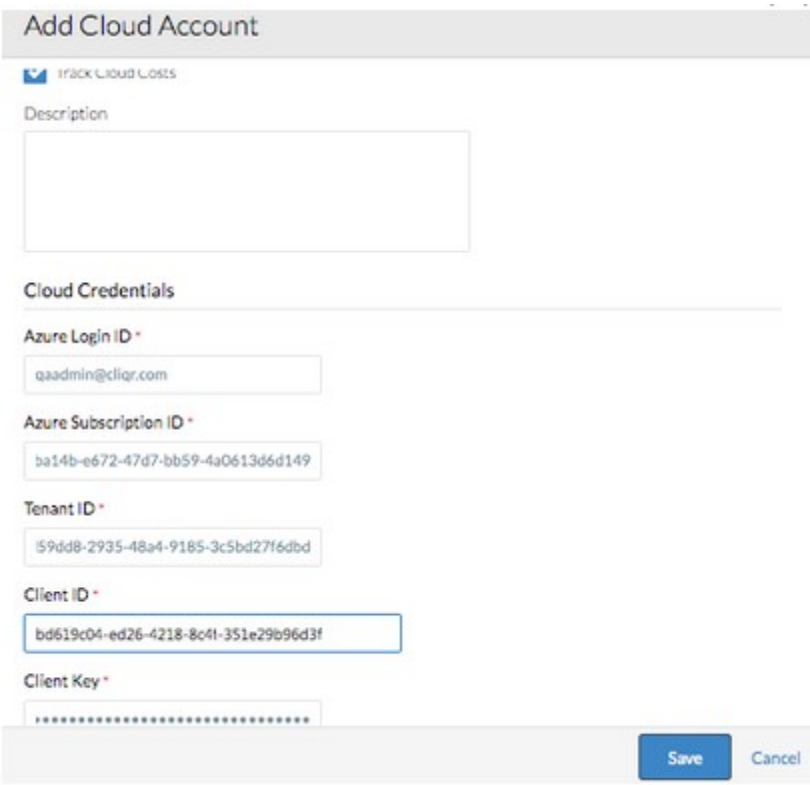
5. [User] 検索ボックスに、あらかじめ定義している Web アプリケーションの名前を入力します。この例では、**CliQrCCO** です。
6. [OK] をクリックして設定内容を保存します。

設定プロセス

Azure Resource Manager クラウドで論理マッピングを設定するには、次の手順に従います。

1. 側面パネルで CCM UI > [管理（Admin）] > [クラウド（Clouds）] > [クラウドの追加（Add Cloud）] にアクセスします。

2. [Microsoft Azure RM] オプションを選択し、このクラウドの名前と説明を入力して、[保存(Save)] をクリックします。
3. 新たに追加されたクラウドを見つけて [クラウド アカウントの追加(Add Cloud Account)] リンクをクリックします。[クラウド アカウントの追加(Add Cloud Account)] ポップアップが表示されます。



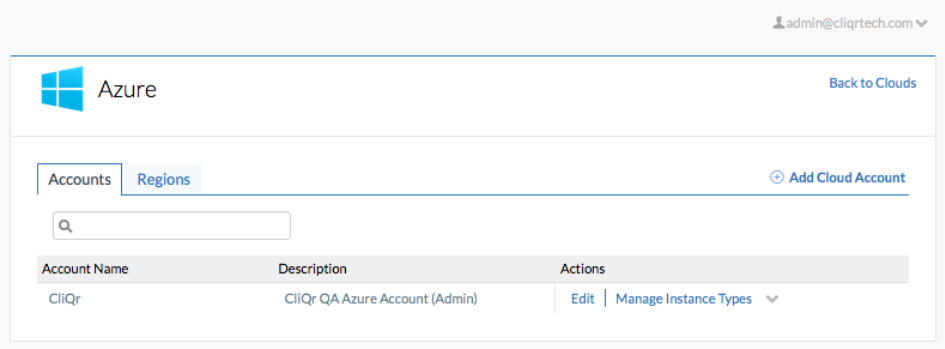
a. 新しいクラウドに名前を割り当てます。

> **ヒント**
> 名前には、スペース、ダッシュ、特殊文字を含めることはできません。

b. Azure アカウントに関連付けられている次のクラウド クレデンシャルを追加します。
   i. Azure ログイン ID(Azure Login ID):Azure Resource Manager クラウド アカウントへのログインに使用される電子メールアドレス
   ii. Azure サブスクリプション ID(Azure Subscription ID):**サブスクリプション ID** を取得するには、上記の「*前提条件*」の項の説明に従って **Azure Classic ポータル**のインターフェイスに切り替えて、[Settings] にアクセスします。

iii. テナント ID(Tenant ID):上記の「*前提条件*」の項の、*エンドポイントの表示*に関する箇条書きで指定されている UUID。
iv. クライアント ID(Client ID):上記の「*前提条件*」の項の、青色のアイコンに関する箇条書きで指定されている UUID。
v. クライアント キー(Client Key):上記の「*前提条件*」の項の、*キー*に関する箇条書きで指定されています。

c. [保存(Save)] をクリックし、新しく追加したクラウド アカウント(用語の詳細な説明は「Cloud」を参照)が [クラウド(Cloud)] ページに表示されていることを確認します。
d. [クラウドの設定(Configure Cloud)] リンクをクリックします。[クラウド アカウント(Cloud Accounts)] ページの [アカウント(Accounts)] タブに、設定したすべてのクラウド アカウントが表示されます。



4. [リージョン(Region)] タブをクリックし、クラウド リージョンを追加します。
   a. [クラウド リージョンの追加(Add Cloud Region)] をクリックします。
   b. このクラウドに必要なリージョンを選択します。
   c. このクラウド リージョンの [リージョン名(Region Name)] およびオプションの [表示名(Display Name)] を追加します。
   d. [保存(Save)] をクリックします。

> インスタンス タイプ、ストレージ タイプ、およびイメージ マップのセクションは、リージョンを追加するとすぐに自動的に設定されます。

5. (任意)[クラウド設定の編集(Edit Cloud Settings)] リンクをクリックし、各クラウド リージョンの必要な設定を更新します。

> CloudCenter の熟練者のアドバイスによる場合を除き、デフォルト値を使用し、変更を行うことは避けてください。

> **注意**
> **クラウド設定を編集**する場合、変更を CCO に保存し、これらの変更がファイアウォールの設定内の CCO にも反映されるようにする必要があります。
>
> CCO がすでに設定されている場合は、これらのクラウド設定を有効にするために CCO を再登録する必要があります。

   a. Azure Resource Manager Url:AzureRM のサービス エンドポイント。非政府向けクラウドおよび非中国向けクラウドのリージョン、つまり URL は、https://management.azure.com/ です。
   b. Azure Active Directory Url:Microsoft により提供され、クレデンシャルを認証するために使用される Azure のアクティブ ディレクトリ URL。非政府向けクラウド、または非中国向けのリージョン、つまり URL は、https://login.microsoftonline.com/ です。
   c. Linux カスタム スクリプト拡張機能のバージョン(Linux Custom Script Extension Version):Microsoft により提供され、動的ブートストラップを実行するためのカスタム スクリプトの拡張。使用するバージョンを指定します。
   d. Windows カスタム スクリプト拡張機能のバージョン(Windows Custom Script Extension Version):Microsoft により提供され、動的ブートストラップを実行するためのカスタム スクリプトの拡張。使用するバージョンを指定します。
   e. Linux 診断拡張機能のバージョン(Linux Diagnostics Extension Version):Microsoft により提供され、メトリック モニタリングを実行するための診断の拡張。使用するバージョンを指定します。
   f. Windows 診断拡張機能のバージョン(Windows Diagnostics Extension Version):Microsoft により提供され、メトリック モニタリングを実行するための診断の拡張。使用するバージョンを指定します。
   g. **[インスタンスの命名方法(Instance Naming Strategy)]**、**[インスタンス IPAM の使用(Instance IPAM Strategy)]**、および [ノード名設定(Node Name Config)]:「VM Name Config」セクションでは、これらの値の設定の詳細を説明しています。
   h. [保存(Save)] をクリックします。

6. クラウド設定を完了するには、CCO を CCM に登録する必要があります。
   CCM への CCO の登録

CCM への CCO の登録

- クラウド リージョンの微妙な違い
- 非 HA モード
- HA モード

クラウド リージョンの微妙な違い

CCM に CCO を登録すると、CCO は登録されたクラウド リージョンにのみ動作します。

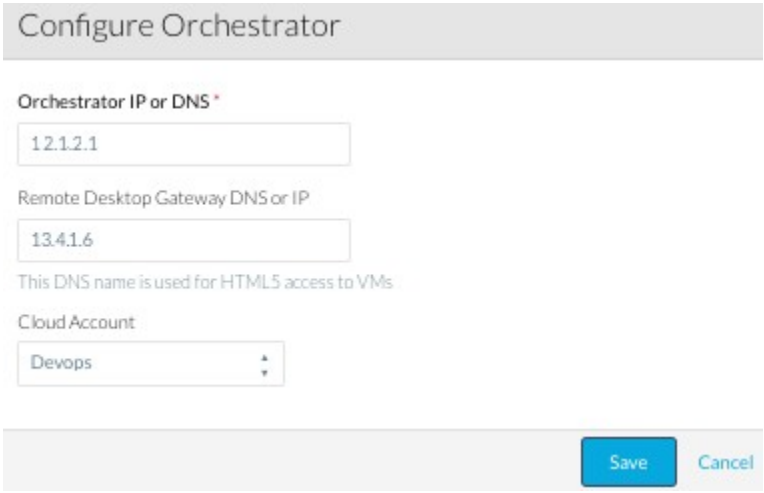
> **CloudCenter**
> CCM に CCO を登録すると、CloudCenter プラットフォームは、このクラウド リージョンがアクティブであると見なし、特定条件下でしか CloudCenter プラットフォームからこのクラウド リージョンを削除できなくなります。詳細については、「Cloud Region Configuration」>「*Delete Cloud Region*」を参照してください。

> 提供された例では AWS クラウドを参照していますが、スクリーン キャプチャはクラウドごとに異なることがある点に注意してください。

非 HA モード

CCM に CCO を登録するには、次の手順に従います。

a. [オーケストレータの設定(Configure Orchestrator)] ポップアップで、CCM からアクセス可能な CCO の IP アドレスを入力し、CCO をホストするために使用されるクラウド アカウントを選択します。



b. このページがまだ表示されていない場合は、必要なクラウドにおいて、[管理(Admin)] > [クラウド(Clouds)] > [リージョンの設定(Configure Regions)] を選択していることを確認します。
   i. [リージョン(Regions)] タブの [オーケストレータの設定(Configure Orchestrator)] をクリックします。
   ii. オーケストレータの IP または DNS(Orchestrator IP or DNS):CCO サーバの IP または DNS アドレスを指定します。
   iii. リモート デスクトップ ゲートウェイの DNS または IP(Remote Desktop Gateway DNS or IP):Guacamole サーバの IP アドレス(VM へのブラウザベースのアクセスを有効化)。Guacamole コンポーネントが AMQP サーバ内に存在している場合は、AMQP サーバの IP アドレスを指定します。
   iv. クラウド アカウント(Cloud Account):この CCO で使用するクラウド アカウントを選択します。

> **Amazon クラウドの微妙な違い**
> IAM ロールを設定している場合、この設定は重要です。必ずこのロールを含むクラウド アカウントを選択してください。

c. [保存(Save)] をクリックします。これで、CCM と CCO の相互信頼関係が確立されました。CloudCenter プラットフォームは現在、導入された CCO によりクラウド リージョンを管理しています。
d. 手順 2 と手順 3 を繰り返し、CCM とその他の CCO 間の相互信頼を確立します。

CCO VM を登録し、設定が完了しました。ここでは、2 つのオプションがあります。

- その他のクラウド リージョンを追加し、これらのクラウドごとに CCO を登録します。詳細については、「クラウド リージョンごと（必須）」を参照してください。
- イメージをマッピングします。詳細については、「イメージ マッピング」を参照してください。

> クラウド アカウントのイメージを起動するアクセス許可を付与する必要がある場合は、「Image Launch Permissions」を参照してください。

- アプリケーションのモデリング、展開、および管理を行います。詳細については、「Application Profile」を参照してください。

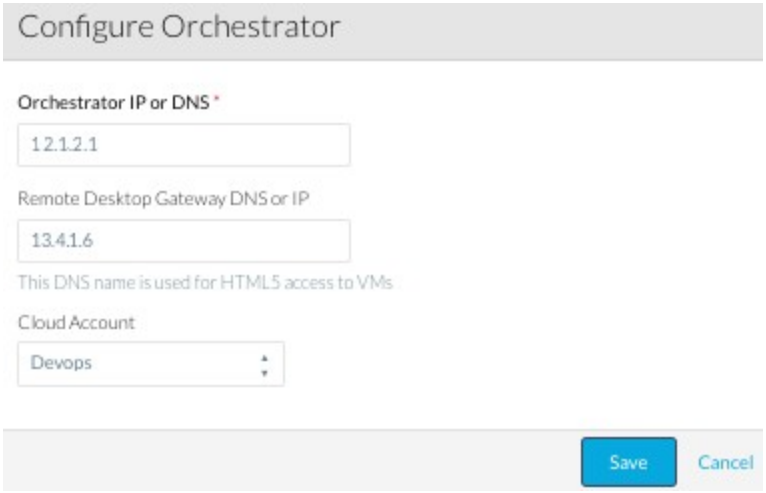
HA モード

CCM に CCO を登録するには、次の手順に従います。

a. プライマリ CCO で Tomcat Service が実行中であることを確認します。
b. セカンダリ CCO およびターシャリ CCO にログインし、両方のサーバで Tomcat Service を停止します。

```
/etc/init.d/tomcat stop
```

c. CCM UI にアクセスし、CCO LB の IP アドレスを使用して CCO を登録します。
   i. このページがまだ表示されていない場合は、必要なクラウドにおいて、[管理（Admin）] > [クラウド（Clouds）] > [リージョンの設定（Configure Regions）] を選択していることを確認します。
   ii. [リージョン（Regions）] タブの [オーケストレータの設定（Configure Orchestrator）] をクリックします。
   iii. CCM からアクセス可能な CCO の IP アドレスを入力し、CCO をホストするために使用されるクラウド アカウントを選択します。



      1. オーケストレータの IP または DNS（Orchestrator IP or DNS）：CCO サーバの IP または DNS アドレスを指定します。
      2. リモート デスクトップ ゲートウェイの DNS または IP（Remote Desktop Gateway DNS or IP）：Guacamole サーバの IP アドレス（VM へのブラウザベースのアクセスを有効化）。Guacamole コンポーネントが AMQP サーバ内に存在している場合は、AMQP サーバの IP アドレスを指定します。
      3. クラウド アカウント（Cloud Account）：この CCO で使用するクラウド アカウントを選択します。必ずこのロールを含むクラウド アカウントを選択してください。
      4. [保存（Save）] をクリックします。これで、CCM と CCO の相互信頼関係が確立されました。CloudCenter プラットフォームは現在、導入された CCO によりクラウド リージョンを管理しています。

d. 登録が成功したら、プライマリ CCO サーバにログインします。
e. プライマリ CCO の **/usr/local/osmosix/etc/** フォルダから、セカンダリ CCO およびターシャリ CCO の両サーバ上の**同じ場所**に **gateway_config.properties** ファイルをコピーします。
f. すべてのサーバのコピーしたファイルの所有権およびアクセス許可が次のようになっていることを確認します。
   - オーナー（Owner）= cliqruser
   - グループ権限（Group Permission）= 読み取りおよび書き込み
g. 必要な場合は、次のコマンドを実行して設定を変更します。

```
chown
cliqruser:cliqruser
/usr/local/osmosix/etc/gateway_config.properties
chmod 644 /usr/local/osmosix/etc/gateway_config.properties
```

h. 各サーバで次のコマンドを発行することによって、セカンダリ CCO とターシャリ CCO サーバで Tomcat を起動します。

```
/etc/init.d/tomcat start
```

i. HA モードのその他の CCO についてこの手順を繰り返し、CCM とその他の CCO 間の相互信頼を確立します。

CCO VM を登録し、設定が完了しました。ここでは、2 つのオプションがあります。

- その他のクラウド リージョンを追加し、これらのクラウドごとに CCO を登録します。詳細については、「クラウド リージョンごと(必須)」を参照してください。
- イメージをマッピングします。詳細については、「イメージ マッピング」を参照してください。

  クラウド アカウントのイメージを起動するアクセス許可を付与する必要がある場合は、「Image Launch Permissions」を参照してください。

- アプリケーションのモデリング、展開、および管理を行います。詳細については、「Application Profile」を参照してください。

戻る:クラウドの設定

- Azure Pack クラウドの設定

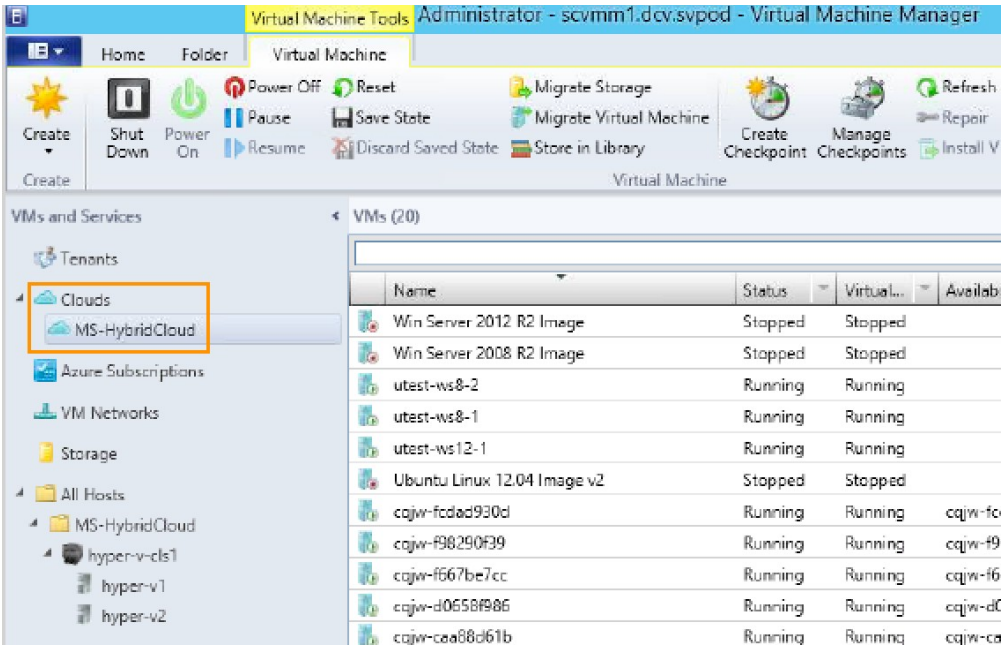
Azure Pack クラウドの設定

次のスクリーン キャプチャは、Azure ポータルが変更されると変わる可能性があることに注意してください。この項ではあくまでも参考として示しています。

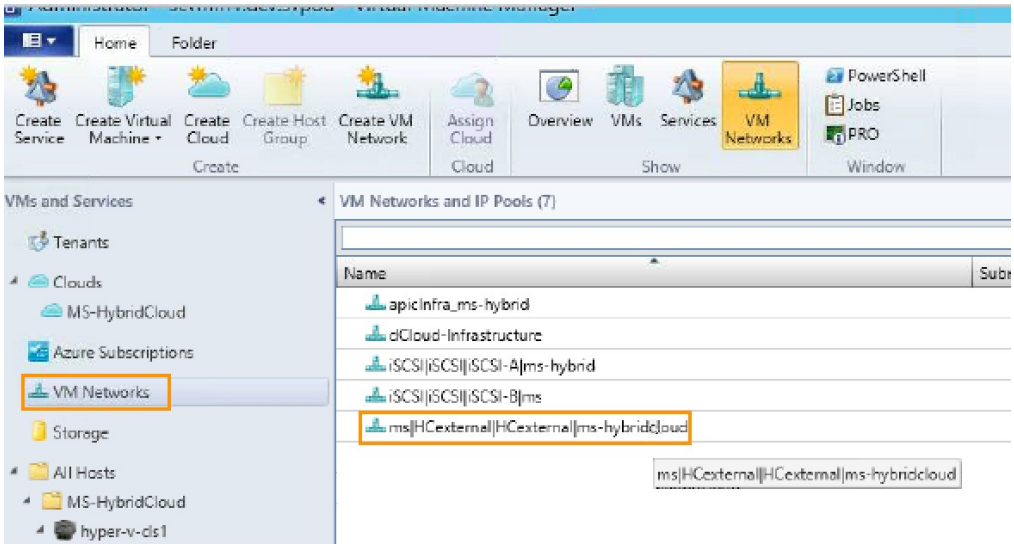
前提条件

CloudCenter プラットフォームで Azure Pack クラウドをマッピングする前に、次の Azure Pack 要件を確認します。

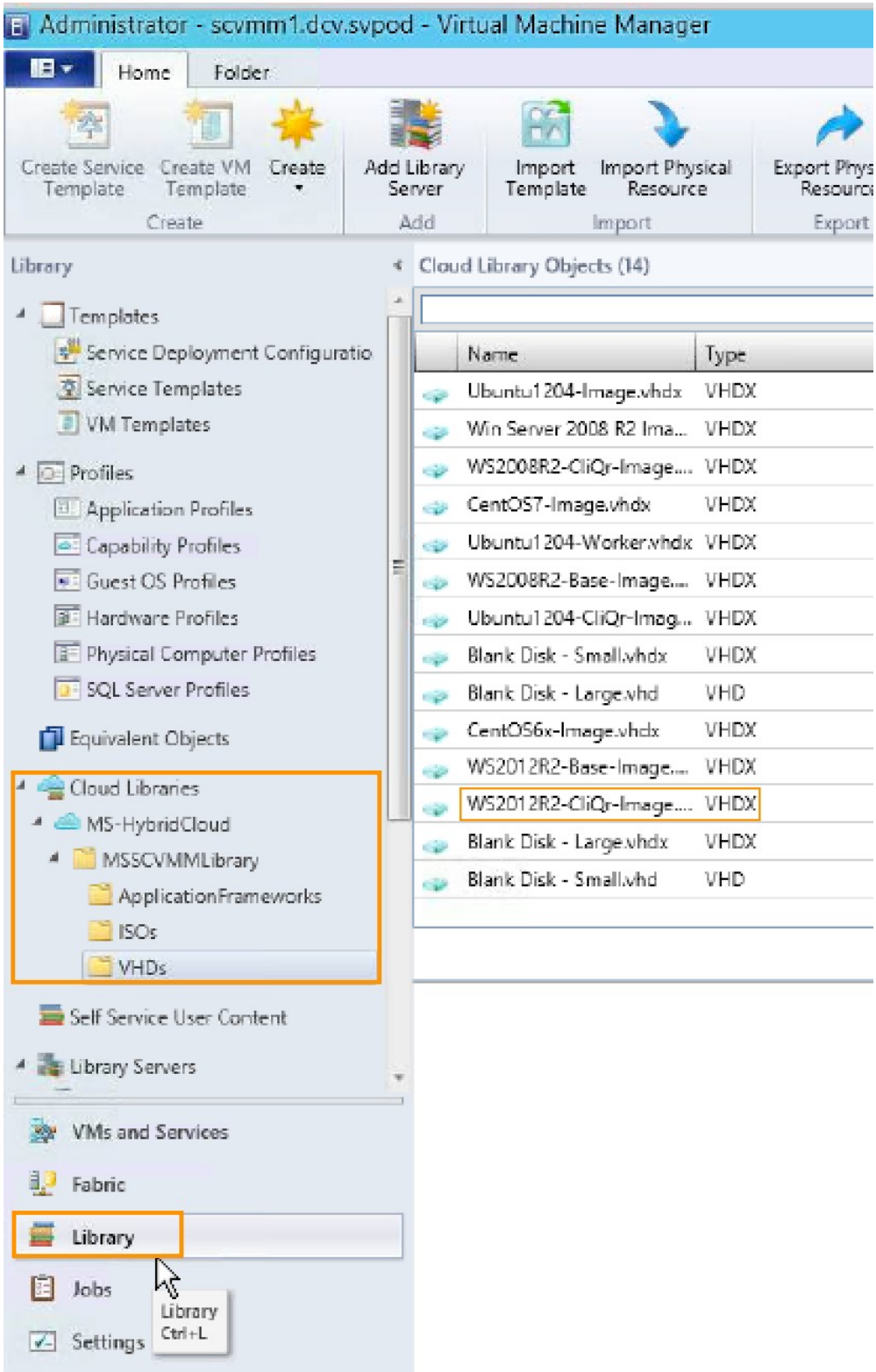
- 以下にアクセスできる有効な Windows Azure Pack アカウント:
  - Azure Pack コンソール:Azure Pack サービス管理ポータル
  - SCVMM:System Center Virtual Machine Manager コンソール
- Azure Pack クラウド アカウント、ネットワーク、およびイメージ。これらの要件が設定されていない場合は、RDP 経由で **SCVMM** Administrator に接続してここで設定します。
  - Azure Pack クラウド(**クラウド アカウント**):



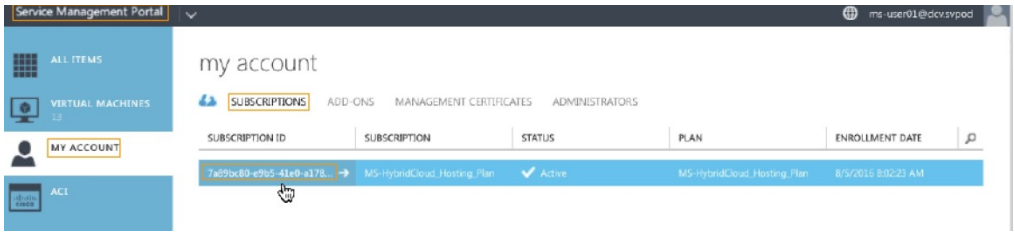
- Azure Pack VM ネットワーク（**ネットワーク**）:



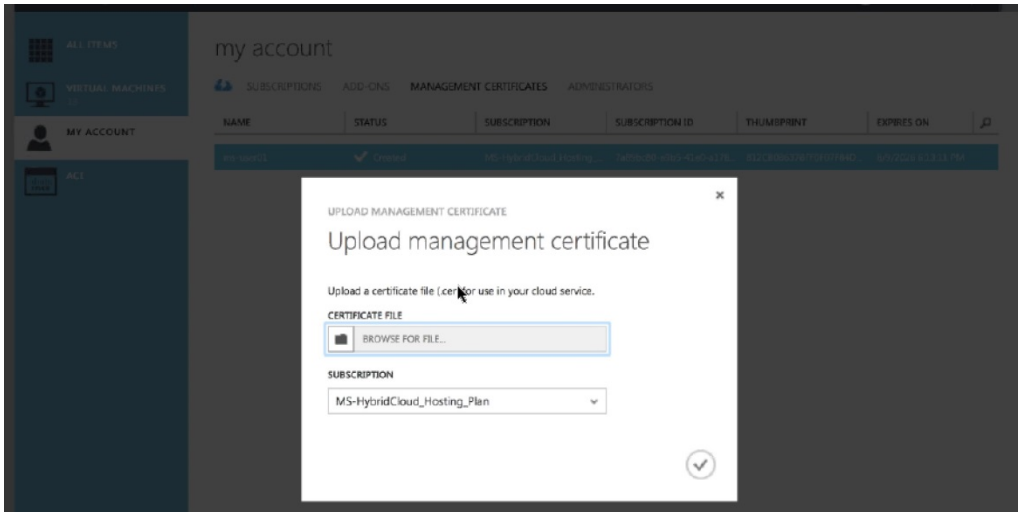
- 各 OS に 1 つの Azure Pack クラウド ライブラリ VHDX イメージ（**イメージ**）:CloudCenter のカスタム イメージのインストールにはこれらのカスタム イメージを含める必要があります。



- Azure Pack ログイン ID とサブスクリプション ID：これらの ID を準備します。これらの ID が準備できていない場合は、**Azure Pack サービス管理ポータル**にアクセスしてこれらを確認します。
  - **Azure Pack ログイン ID**：Azure Pack サービス管理ポータルにアクセスするために使用する ID。
  - **Azure Pack サブスクリプション ID**：次のページのサブスクリプション ID。



- **管理証明書**:Azure コンソール > [Settings] > [Manage Certificates] にアクセスし、(シスコによって生成される)azure-certificate.cer ファイルをアップロードします。



- このアカウントの SSH キーと管理証明書。

> MacPort からのものでない OpenSSL、特に OpenSSL 1.0.1f 6 Jan 2014 は、有効な SSH キー ペアを作成しない傾向があることに注意してください。他のオプションとしては、FWIW、Ubuntu 12.04 LTS 上の OpenSSL 1.0.1c 10 May 2012 があります。

- OpenSSL を使用して SSH キーを生成します。

```
# You may want to use another dir than /tmp
cd /tmp
openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout
azure-
private.key -out azure-certificate.pem
chmod 600 azure-private.key azure-certificate.pem
openssl x509 -outform der -in azure-certificate.pem -out
azure-
certificate.cer
```

- すべての Azure API コール用の証明書で、認証のためにプラグインによって使用されるキーストアを生成します。

```
# Generate a keystore (azurekeystore.pkcs12)
# Transform private key to PEM format
openssl pkcs8 -topk8 -nocrypt -in azure-private.key -inform
PEM -out azure-pk.pem -outform PEM
# Transform certificate to PEM format
openssl x509 -inform der -in azure-certificate.cer -out
azure-cert.pem
cat azure-cert.pem azure-pk.pem > azure.pem.txt
# You MUST enter a password!
openssl pkcs12 -export -in azure.pem.txt -out
azurekeystore.pkcs12 -name
azure -noiter -nomaciter
```

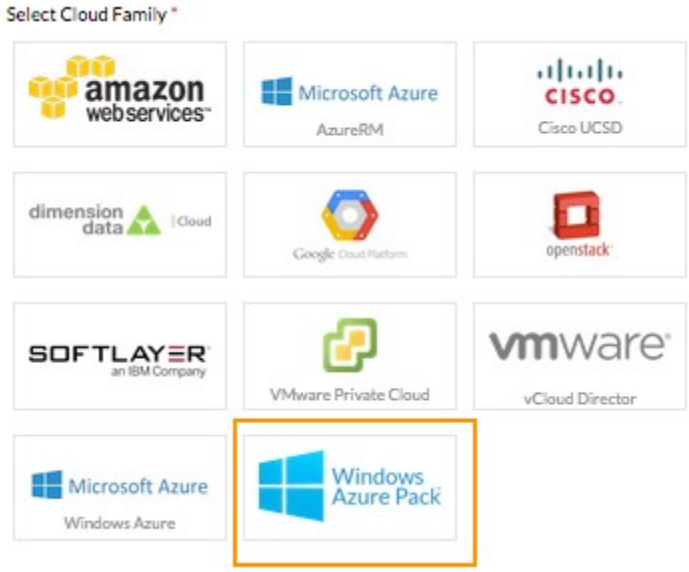
[Upload Management Certificate] ダイアログの情報を入力し、完了の**チェックマーク**を押します。

> CCM UI で Azure Pack リージョンを作成する場合、これらのファイルを Azure にアップロードして、ローカル デバイスまたはそこから簡単にファイルをコピーできるデバイスでコマンドを実行できるようにする必要があります。

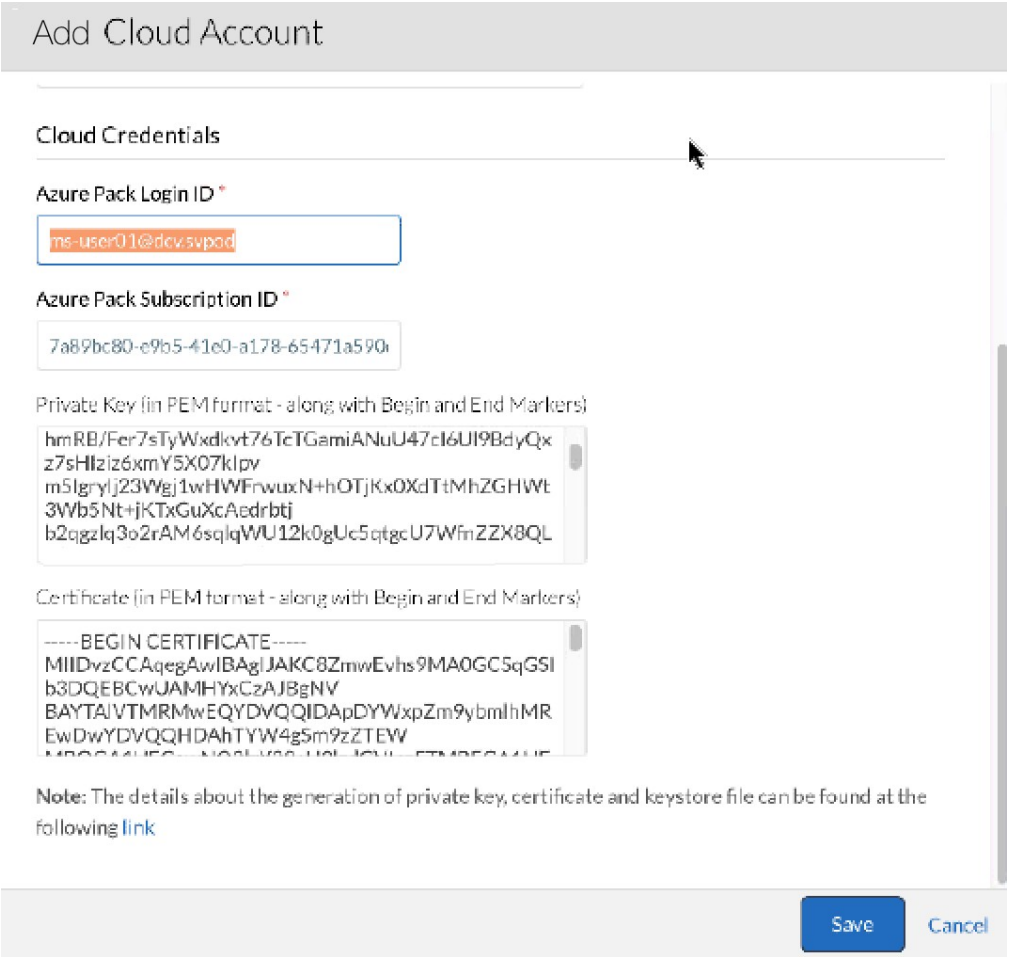
設定プロセス

Azure Pack クラウドで論理マッピングを設定するには、次の手順に従います。

1. CCM UI にアクセスし、CCM UI のメインメニューで [管理(Admin)] > [クラウド(Clouds)] > [クラウドの追加(Add Cloud)] を選択します。



2. [Microsoft Azure Pack] オプションを選択し、このクラウドの名前と説明を入力して、[保存(Save)] をクリックします。
3. 新たに追加されたクラウドを見つけて [クラウド アカウントの追加(Add Cloud Account)] リンクをクリックします。[クラウド アカウントの追加(Add Cloud Account)] ポップアップが表示されます。



a. 新しいクラウドに名前を割り当てます。

> **ヒント**
> 名前には、スペース、ダッシュ、特殊文字を含めることはできません。

b. Azure Pack アカウントに関連付けられている次のクラウド クレデンシャルを追加します。
   i. Azure Pack ログイン ID（Azure Pack Login ID）：Azure Pack クラウド アカウントへのログインに使用される電子メールアドレス
   ii. Azure Pack サブスクリプション ID（Azure Pack Subscription ID）：**サブスクリプション ID** を取得するには：

   iii. テナント ID（Tenant ID）：上記の「*前提条件*」の項の、*エンドポイントの表示*に関する箇条書きで指定されている UUID。
   iv. PEM 形式の秘密キー（Private Key in PEM Format）：この手順の最初の「*前提条件*」セクションで指定されている **Azure Pack サービス管理ポータル**のキー情報をコピーして貼り付けます。
   v. PEM 形式の証明書（Certificate in PEM Format）：この手順の最初の「*前提条件*」セクションで指定されている **Azure Pack サービス管理ポータル**の証明書情報をコピーして貼り付けます。

4. [リージョン（Region）] タブをクリックし、クラウド リージョンを追加します。
   a. [クラウド リージョンの追加（Add Cloud Region）] をクリックします。
   b. このクラウドに必要なリージョンを選択します。
   c. このクラウド リージョンの [リージョン名（Region Name）] およびオプションの [表示名（Display Name）] を追加します。
   d. [保存（Save）] をクリックします。
5. [クラウド設定の編集（Edit Cloud Settings）] リンクをクリックし、各クラウド リージョンの必要な設定を構成します。

CloudCenter の熟練者のアドバイスによる場合を除き、デフォルト値を使用し、変更を行うことは避けてください。

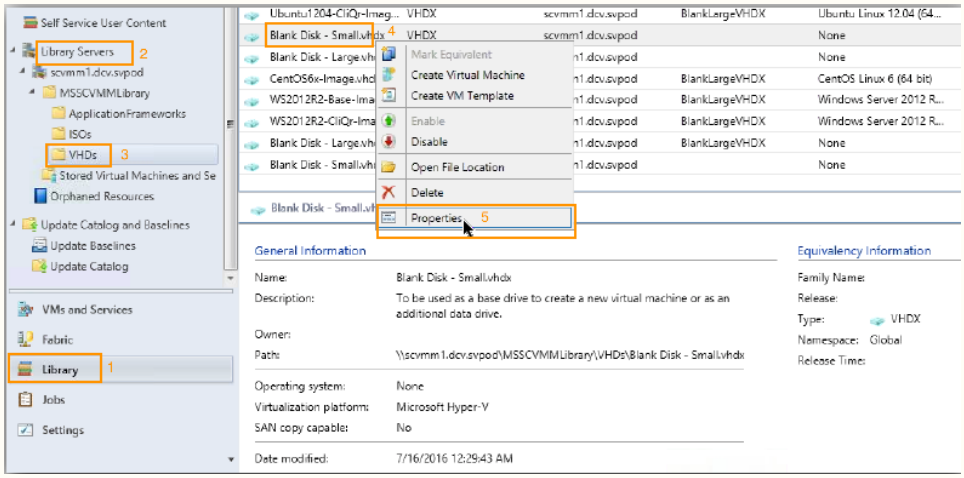
- Azure Pack ネットワーク(Azure Pack Network):上記の「*前提条件*」セクションで指定されている SCVMM コンソールの Azure Pack VM ネットワーク(**ネットワーク**)のリスト。SCVMM コンソールに表示されるとおりに名前を正確にコピーして、このフィールドに貼り付けます。
- Azure Pack データ ディスク(Azure Pack Data Disk):上記の「*前提条件*」セクションで指定されている SCVMM コンソールの Azure Pack クラウド ライブラリ VHDX(**イメージ**)データ ディスクのリスト。

このデータ ディスク設定は、追加のボリュームを設定する場合にのみ必要です。

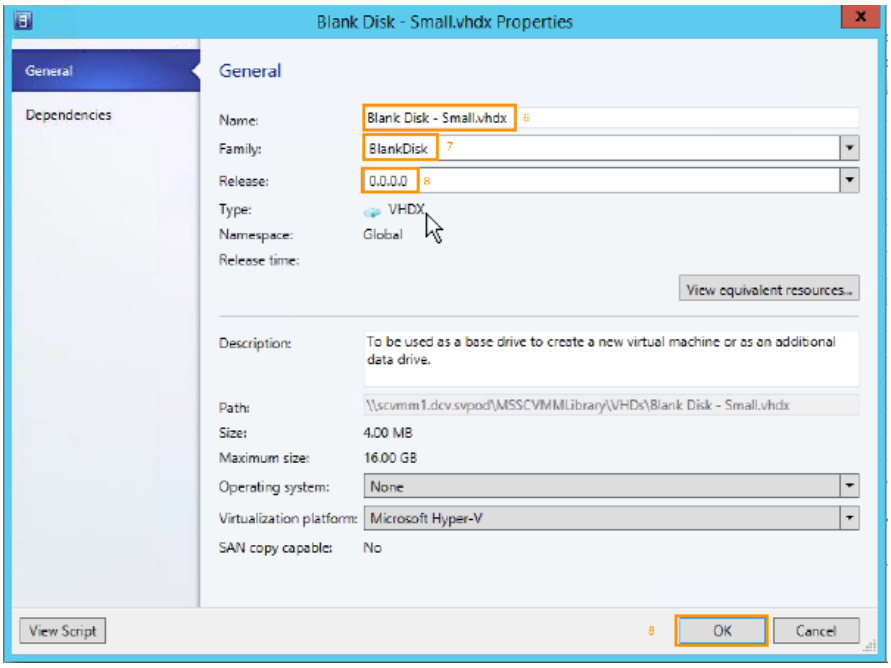
イメージ マッピング

空のディスク用の手順

Azure Pack では、複数のボリュームをサービス プロパティ([一般設定(General Settings)])[デフォルト ボリューム サイズ(Default Volume Size)] フィールドに指定できません。代わりに、次のように空のディスク(サイズを変更することはできません)を使用する必要があります。



a. SCVMM コンソールの Azure Pack クラウド **ライブラリ**にアクセスします
b. ライブラリ サーバをクリックします
c. VHDX フォルダをクリックします
d. 必要な空のディスクを特定します。
e. この空のディスクを右クリックし、[プロパティ(Properties)] を選択します。この空のディスクの [プロパティ(Properties)] ポップアップが表示されます。



f. 名前が自動的に表示されます。
g. [ファミリ(Family)] フィールドで、任意の名前を割り当てる***必要があります***。この形式を指定しない場合、設定は正常に完了しません。

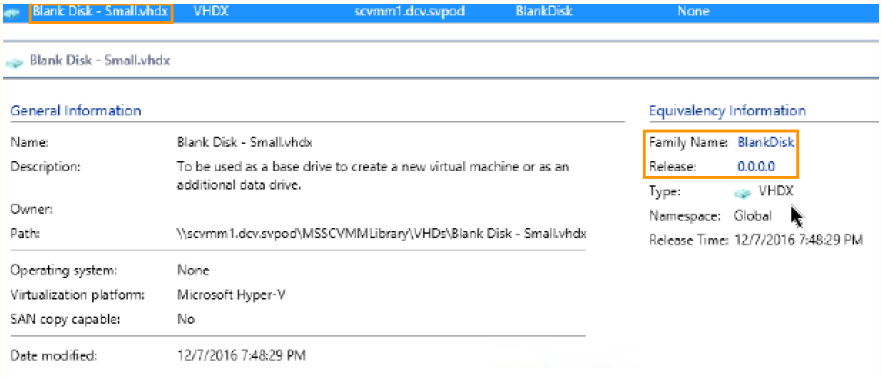
h. [リリース(Release)] フィールドで、*3 つのピリオドで区切られた 4 つの数字*(例:1.2.3.4)を指定する***必要があります***。この正確な形式は、ディスクの識別子として必要です。この形式を指定しない場合、設定は正常に完了しません。

i. [オペレーティング システム(Operating system)] フィールドで、サポートされる正確な OS (Ubuntu 12:04 または CentOS)を選択する***必要があります***。

> この正確な形式は、イメージ マッピングの際に必要です。このフィールドで定められた正確な OS を指定する必要があります。この形式を指定しない場合、イメージ マッピング設定は正常に完了しません。

j. [OK] をクリックして変更を保存します。

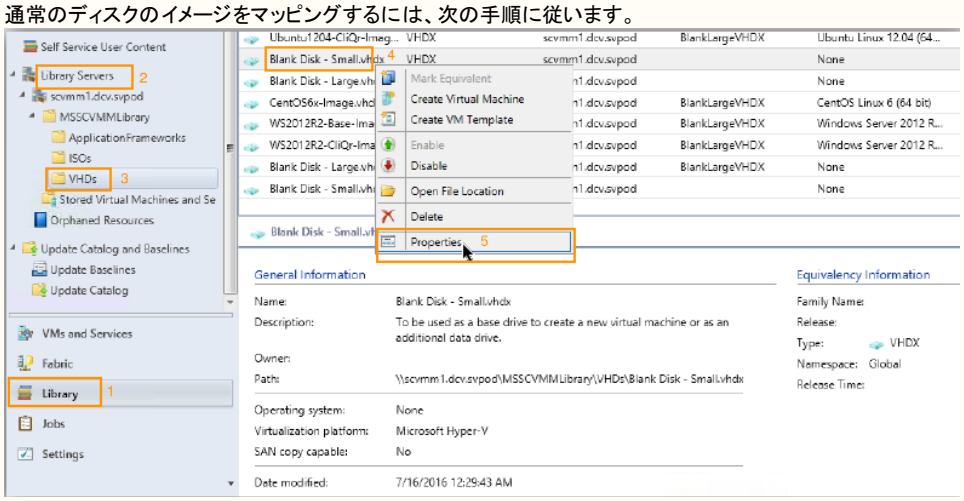
k. SCVMM コンソールの [同等性情報(Equivalency Information)] セクションはこの新しい情報に更新されます。



l. CCM UI の [Azure Pack データ ディスク(Azure Pack Data Disk)] フィールドで、これら 2 つの詳細を次の形式で追加する必要があります。
BlankDisk:0.0.0.0
この形式を指定しない場合、設定は正常に完了しません。

通常のディスク用の手順

通常のディスクのイメージをマッピングするには、次の手順に従います。



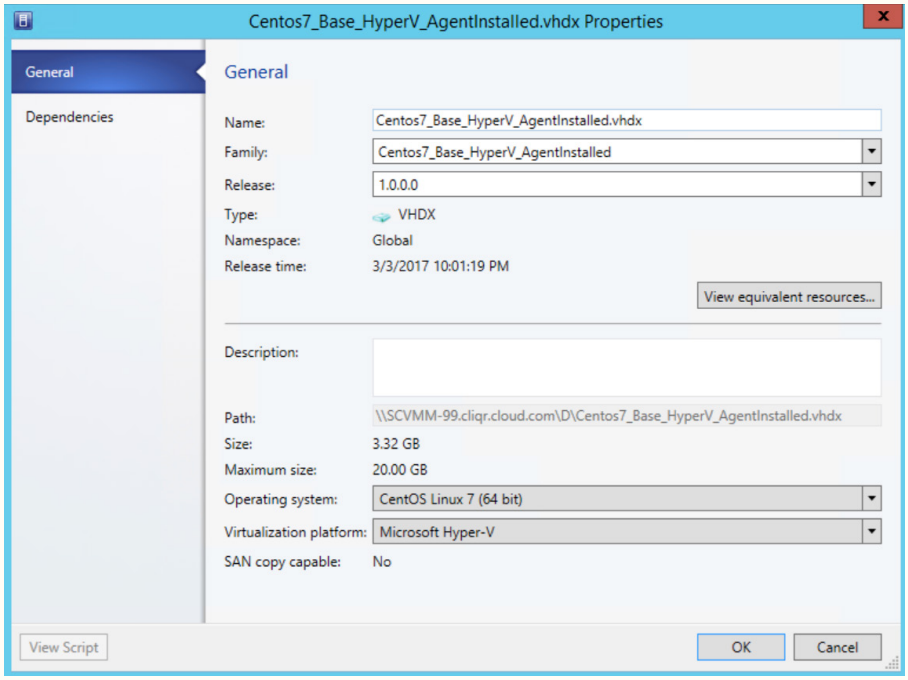
a. SCVMM コンソールの Azure Pack クラウド **ライブラリ**にアクセスします

b. ライブラリ サーバをクリックします

c. VHDX フォルダをクリックします

d. 必要なディスクを特定します。

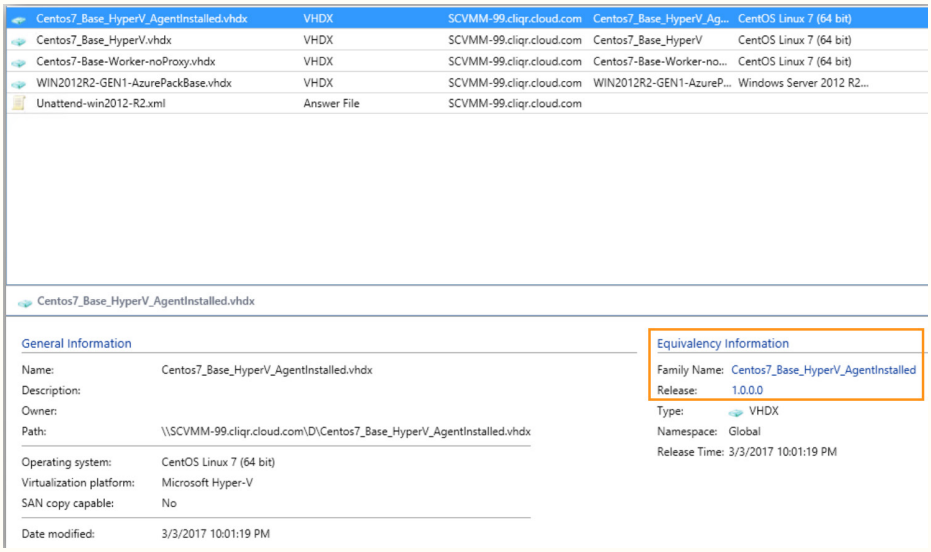
e. このディスクを右クリックし、[プロパティ(Properties)] を選択します。このディスクの [プロパティ(Properties)] ポップアップが表示されます。



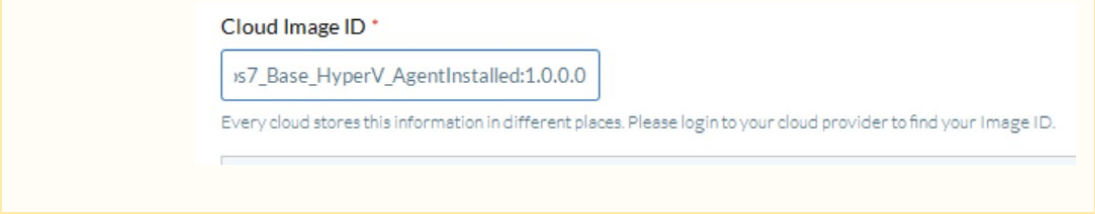
f. 名前が自動的に表示されます。
g. [ファミリ(Family)] フィールドで、任意の名前を割り当てる***必要があります***。この形式を指定しない場合、設定は正常に完了しません。
h. [リリース(Release)] フィールドで、*3 つのピリオドで区切られた 4 つの数字*(例:1.2.3.4)を指定する***必要があります***。この正確な形式は、ディスクの識別子として必要です。この形式を指定しない場合、設定は正常に完了しません。
i. [オペレーティング システム(Operating system)] フィールドで、サポートされる正確な OS(Ubuntu 12:04 または CentOS)を選択する***必要があります***。

> この正確な形式は、イメージ マッピングの際に必要です。このフィールドで定められた正確な OS を指定する必要があります。この形式を指定しない場合、イメージ マッピング設定は正常に完了しません。

j. [OK] をクリックして変更を保存します。
k. SCVMM コンソールの [同等性情報(Equivalency Information)] セクションはこの新しい情報に更新されます。



l. CCM UI の [Azure Pack データ ディスク(Azure Pack Data Disk)] フィールドで、これら 2 つの詳細を次の形式で追加する必要があります。
Exact_Family_Name:Release
この形式を指定しない場合、設定は正常に完了しません。
m. CCM UI で [クラウド イメージ ID(Cloud Image ID)] として ***Exact_Family_Name:Release*** の詳細を追加します。



- エンドポイント（Endpoint）：正確な DNS 名と SCVMM コンソールに使用するポート。
  例：**wap1.dcv.svpod:30006**
- メタデータ サーバ（Metadata Server）：シスコが提供するデフォルトのメタデータ サーバ（**mds.cliqrtech.com**）を使用することも、独自のメタデータ サーバを構築して使用することもできます。
- ドメイン（Domain）：Azure Pack サーバが存在するドメイン。このドメインの正確な名前については、Azure Pack ドメイン管理者に確認してください。

6. クラウド設定を完了するには、CCO を CCM に登録する必要があります。
   CCM への CCO の登録

CCM への CCO の登録

- クラウド リージョンの微妙な違い
- 非 HA モード
- HA モード

クラウド リージョンの微妙な違い

CCM に CCO を登録すると、CCO は登録されたクラウド リージョンにのみ動作します。

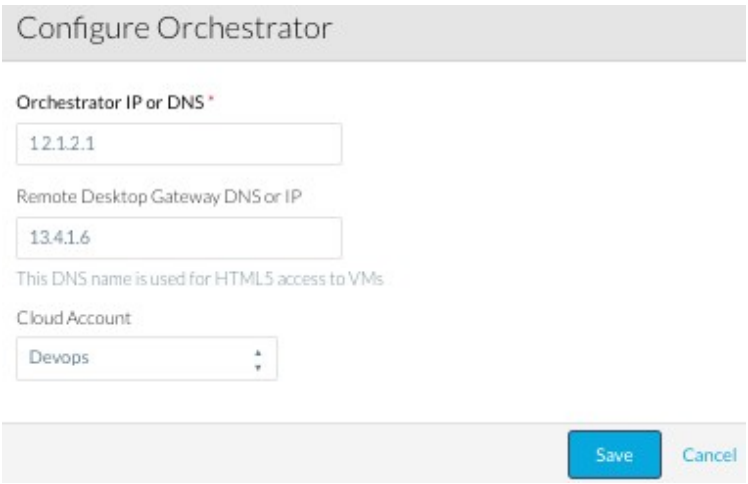
> **CloudCenter**
> CCM に CCO を登録すると、CloudCenter プラットフォームは、このクラウド リージョンがアクティブであると見なし、特定条件下でしか CloudCenter プラットフォームからこのクラウド リージョンを削除できなくなります。詳細については、「Cloud Region Configuration」>「*Delete Cloud Region*」を参照してください。

> 提供された例では AWS クラウドを参照していますが、スクリーン キャプチャはクラウドごとに異なることがある点に注意してください。

非 HA モード

CCM に CCO を登録するには、次の手順に従います。

a. [オーケストレータの設定（Configure Orchestrator）] ポップアップで、CCM からアクセス可能な CCO の IP アドレスを入力し、CCO をホストするために使用されるクラウド アカウントを選択します。



b. このページがまだ表示されていない場合は、必要なクラウドにおいて、[管理（Admin）] > [クラウド（Clouds）] > [リージョンの設定（Configure Regions）] を選択していることを確認します。
   i. [リージョン（Regions）] タブの [オーケストレータの設定（Configure Orchestrator）] をクリックします。
   ii. オーケストレータの IP または DNS（Orchestrator IP or DNS）：CCO サーバの IP または DNS アドレスを指定します。

iii. リモート デスクトップ ゲートウェイの DNS または IP（Remote Desktop Gateway DNS or IP）：Guacamole サーバの IP アドレス（VM へのブラウザベースのアクセスを有効化）。Guacamole コンポーネントが AMQP サーバ内に存在している場合は、AMQP サーバの IP アドレスを指定します。
iv. クラウド アカウント（Cloud Account）：この CCO で使用するクラウド アカウントを選択します。

> **Amazon クラウドの微妙な違い**
> IAM ロールを設定している場合、この設定は重要です。必ずこのロールを含むクラウド アカウントを選択してください。

c. [保存（Save）] をクリックします。これで、CCM と CCO の相互信頼関係が確立されました。CloudCenter プラットフォームは現在、導入された CCO によりクラウド リージョンを管理しています。
d. 手順 2 と手順 3 を繰り返し、CCM とその他の CCO 間の相互信頼を確立します。

CCO VM を登録し、設定が完了しました。ここでは、2 つのオプションがあります。

- その他のクラウド リージョンを追加し、これらのクラウドごとに CCO を登録します。詳細については、「クラウド リージョンごと（必須）」を参照してください。
- イメージをマッピングします。詳細については、「イメージ マッピング」を参照してください。

> クラウド アカウントのイメージを起動するアクセス許可を付与する必要がある場合は、「Image Launch Permissions」を参照してください。

- アプリケーションのモデリング、展開、および管理を行います。詳細については、「Application Profile」を参照してください。

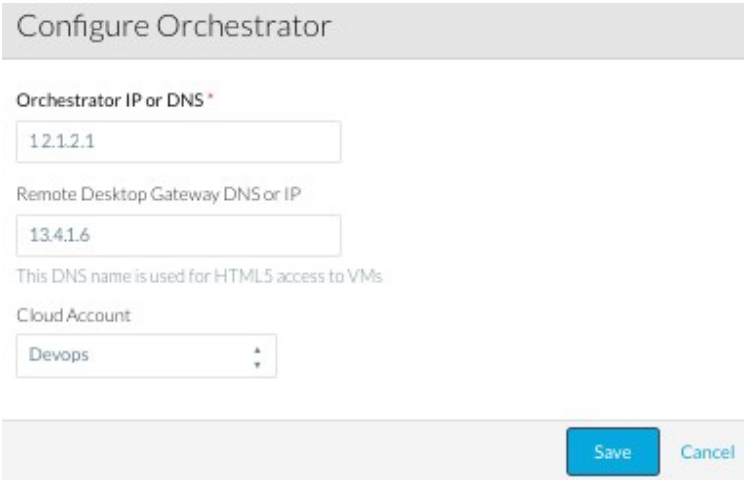
HA モード

CCM に CCO を登録するには、次の手順に従います。

a. プライマリ CCO で Tomcat Service が実行中であることを確認します。
b. セカンダリ CCO およびターシャリ CCO にログインし、両方のサーバで Tomcat Service を停止します。

```
/etc/init.d/tomcat stop
```

c. CCM UI にアクセスし、CCO LB の IP アドレスを使用して CCO を登録します。
   i. このページがまだ表示されていない場合は、必要なクラウドにおいて、[管理（Admin）] > [クラウド（Clouds）] > [リージョンの設定（Configure Regions）] を選択していることを確認します。
   ii. [リージョン（Regions）] タブの [オーケストレータの設定（Configure Orchestrator）] をクリックします。
   iii. CCM からアクセス可能な CCO の IP アドレスを入力し、CCO をホストするために使用されるクラウド アカウントを選択します。



   1. オーケストレータの IP または DNS（Orchestrator IP or DNS）：CCO サーバの IP または DNS アドレスを指定します。
   2. リモート デスクトップ ゲートウェイの DNS または IP（Remote Desktop Gateway DNS or IP）：Guacamole サーバの IP アドレス（VM へのブラウザベースのアクセスを有効化）。Guacamole コンポーネントが AMQP サーバ内に存在している場合は、AMQP サーバの IP アドレスを指定します。
   3. クラウド アカウント（Cloud Account）：この CCO で使用するクラウド アカウントを選択します。必ずこのロールを含むクラウド アカウントを選択してください。
   4. [保存（Save）] をクリックします。これで、CCM と CCO の相互信頼関係が確立されました。CloudCenter プラットフォームは現在、導入された CCO によりクラウド リージョンを管理しています。

d. 登録が成功したら、プライマリ CCO サーバにログインします。
e. プライマリ CCO の **/usr/local/osmosix/etc/** フォルダから、セカンダリ CCO およびターシャリ CCO の両サーバ上の**同じ場所**に **gateway_config.properties** ファイルをコピーします。

f. すべてのサーバのコピーしたファイルの所有権およびアクセス許可が次のようになっていることを確認します。
   - オーナー(Owner)= cliqruser
   - グループ権限(Group Permission)= 読み取りおよび書き込み

g. 必要な場合は、次のコマンドを実行して設定を変更します。

```
chown
cliqruser:cliqruser
/usr/local/osmosix/etc/gateway_config.properties
chmod 644 /usr/local/osmosix/etc/gateway_config.properties
```

h. 各サーバで次のコマンドを発行することによって、セカンダリ CCO とターシャリ CCO サーバで Tomcat を起動します。

```
/etc/init.d/tomcat start
```

i. HA モードのその他の CCO についてこの手順を繰り返し、CCM とその他の CCO 間の相互信頼を確立します。

CCO VM を登録し、設定が完了しました。ここでは、2 つのオプションがあります。

- その他のクラウド リージョンを追加し、これらのクラウドごとに CCO を登録します。詳細については、「クラウド リージョンごと(必須)」を参照してください。
- イメージをマッピングします。詳細については、「イメージ マッピング」を参照してください。

> クラウド アカウントのイメージを起動するアクセス許可を付与する必要がある場合は、「Image Launch Permissions」を参照してください。

- アプリケーションのモデリング、展開、および管理を行います。詳細については、「Application Profile」を参照してください。

戻る:クラウドの設定

- Azure Classic クラウドの設定

Azure Classic クラウドの設定

> 次のスクリーン キャプチャは、Azure ポータルが変更されると変わる可能性があることに注意してください。この項ではあくまでも参考として示しています。

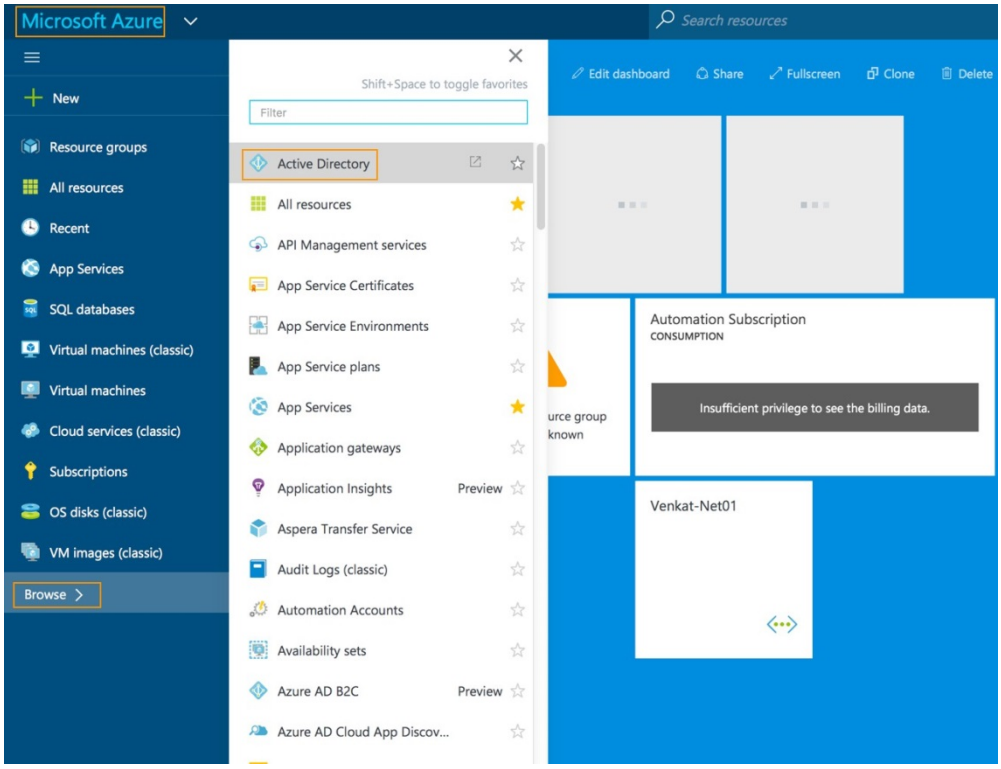
前提条件

Azure Classic クラウドをマッピングする前に、次の前提条件を確認してください。

- 有効な Windows Azure アカウントを持っている。
- 登録済みのプロバイダーを確認するのに ARM(本マニュアルでは Azure Resource Manager を意味する)モードを使用しているかどうかを確認します。この手順では、Azure CLI を使用する必要があります。
  1. Azure CLI をプラットフォームにインストールします。詳細については、https://azure.microsoft.com/en-us/documentation/articles/xplat-cli-install/ を参照してください。
  2. Azure CLI にログ インします。
     azure login
  3. ARM モードを使用していることを確認します。
     azure config mode arm
  4. プロバイダーを登録します。
     azure provider register Microsoft.Compute Microsoft.Storage Microsoft.Network Microsoft.Resources Microsoft.Authorization

     > PowerShell を使用している場合は、次のコマンドを使用してプロバイダーを登録します。
     >
     > **Register-AzureProvider**

  5. これらのプロバイダーが登録されているかどうかを確認します。
     azure provider list
- **Azure Classic ポータル**のインターフェイスは Azure Resource Manager のインターフェイスと異なります。Azure Classic ポータルの Active Directory にアクセスするには、次の図を参照してください。



- このアカウントの SSH キーと管理証明書。

> ⚠ MacPort からのものでない OpenSSL、特に OpenSSL 1.0.1f 6 Jan 2014 は、有効な SSH キー ペアを作成しない傾向があることに注意してください。他のオプションとしては、FWIW、Ubuntu 12.04 LTS 上の OpenSSL 1.0.1c 10 May 2012 があります。

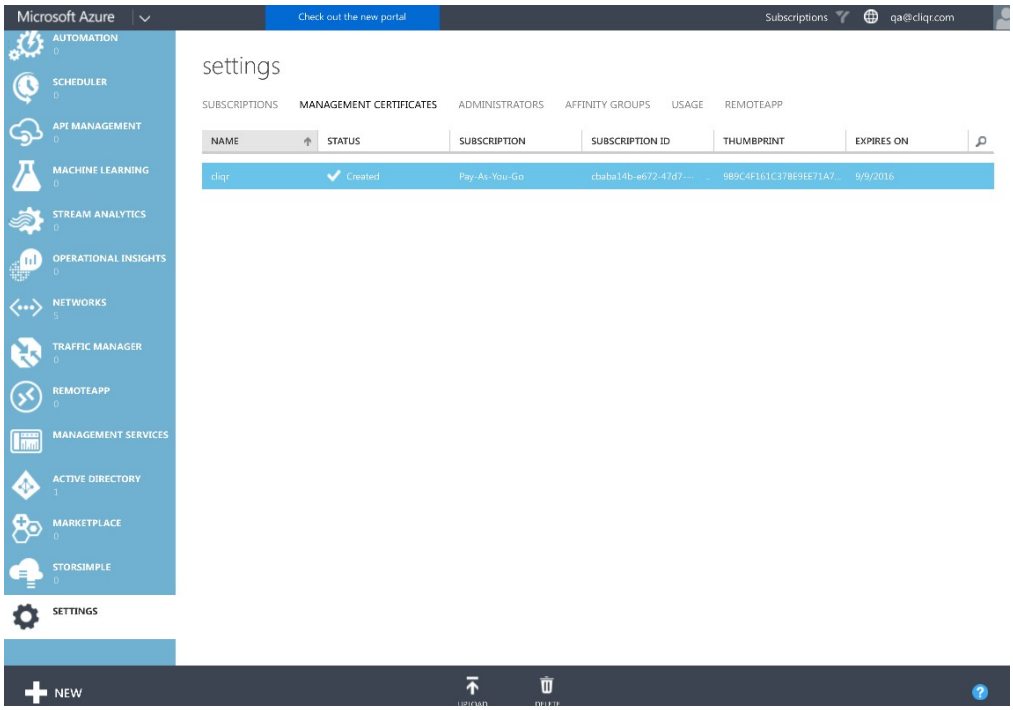
- OpenSSL を使用して SSH キーを生成します。

```
# You may want to use another dir than /tmp
cd /tmp
openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout
azure- private.key -out azure-certificate.pem
chmod 600 azure-private.key azure-certificate.pem
openssl x509 -outform der -in azure-certificate.pem -out
azure- certificate.cer
```

- すべての Azure API コール用の証明書で、認証のためにプラグインによって使用されるキーストアを生成します。

```
# Generate a keystore (azurekeystore.pkcs12)
# Transform private key to PEM format
openssl pkcs8 -topk8 -nocrypt -in azure-private.key -inform PEM -
out azure-pk.pem -outform PEM
# Transform certificate to PEM format
openssl x509 -inform der -in azure-certificate.cer -out azure-
cert.pem cat azure-cert.pem azure-pk.pem > azure.pem.txt
# You MUST enter a password!
openssl pkcs12 -export -in azure.pem.txt -out azurekeystore.pkcs12 -
name azure -noiter -nomaciter
```

- [Azure Console] > [Settings] > [Manage Certificates] を選択して、azure-certificate.cer ファイル（Cisco 作成）をアップロードします。

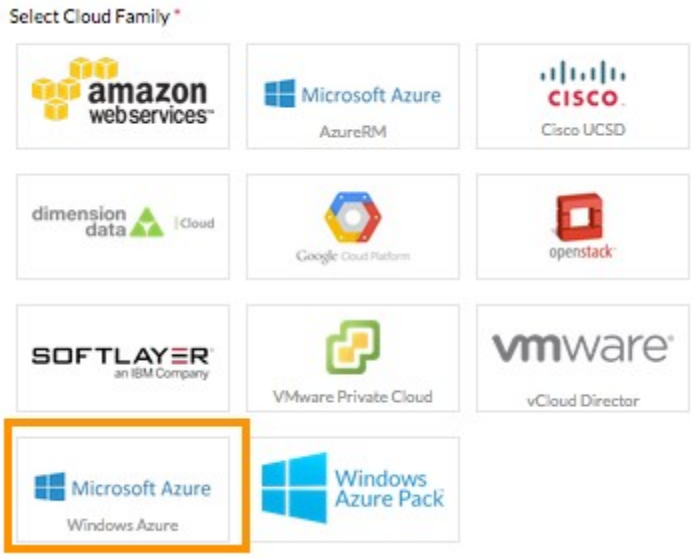


CCM UI で Azure リージョンを作成する場合、これらのファイルを Azure にアップロードして、ローカル デバイスまたはそこから簡単にファイルをコピーできるデバイスでコマンドを実行できるようにする必要があります。

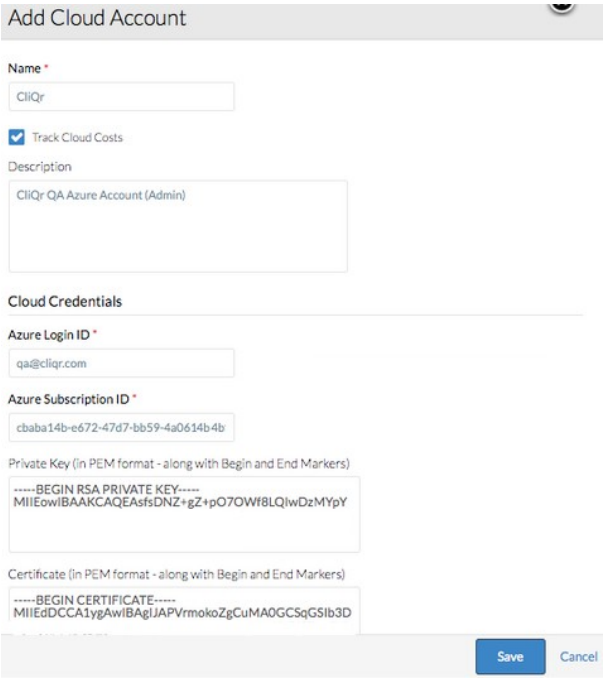
設定プロセス

Azure クラウドで論理マッピングを設定するには、次のプロセスに従ってください。

1. CCM UI にアクセスし、CCM UI のメインメニューで [管理(Admin)] > [クラウド(Clouds)] > [クラウドの追加(Add Cloud)] を選択します。



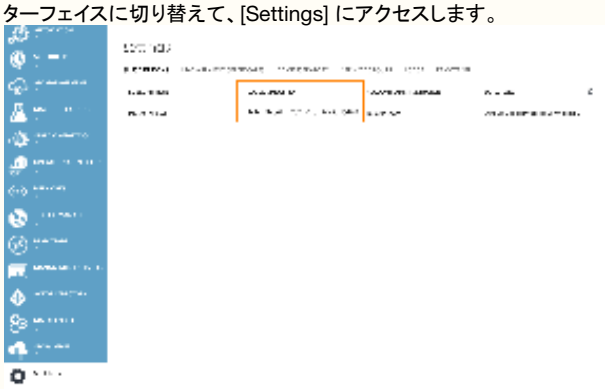
2. [Microsoft Windows Azure] オプションを選択し、このクラウドの名前と説明を入力して、[保存(Save)] をクリックします。
3. 新たに追加されたクラウドを見つけて [クラウド アカウントの追加(Add Cloud Account)] リンクをクリックします。[クラウド アカウントの追加(Add Cloud Account)] ポップアップが表示されます。



a. 新しいクラウドに名前を割り当てます。

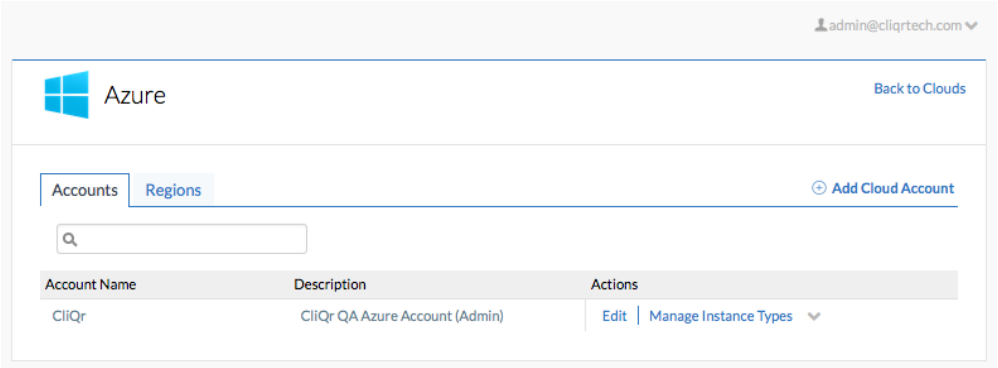
> **ヒント**
> 名前には、スペース、ダッシュ、特殊文字を含めることはできません。

b. Azure アカウントに関連付けられたクラウド クレデンシャル（ログイン ID、サブスクリプション ID、プライベート キー、および証明書）を追加します。この手順の開始時に、「*前提条件*」の項で指定した PEM および証明書のテキストをコピー アンド ペーストします。

> **サブスクリプション ID** を取得するには、上記の「*前提条件*」の項の説明に従って **Azure Classic ポータル**のインターフェイスに切り替えて、[Settings] にアクセスします。
>
> 

c. [保存（Save）] をクリックし、新しく追加したクラウド アカウント（用語の詳細な説明は「Cloud」を参照）が [クラウド（Cloud）] ページに表示されていることを確認します。

d. [クラウドの設定（Configure Cloud）] リンクをクリックします。[クラウド アカウント（Cloud Accounts）] ページの [アカウント（Accounts）] タブに、設定したすべてのクラウド アカウントが表示されます。

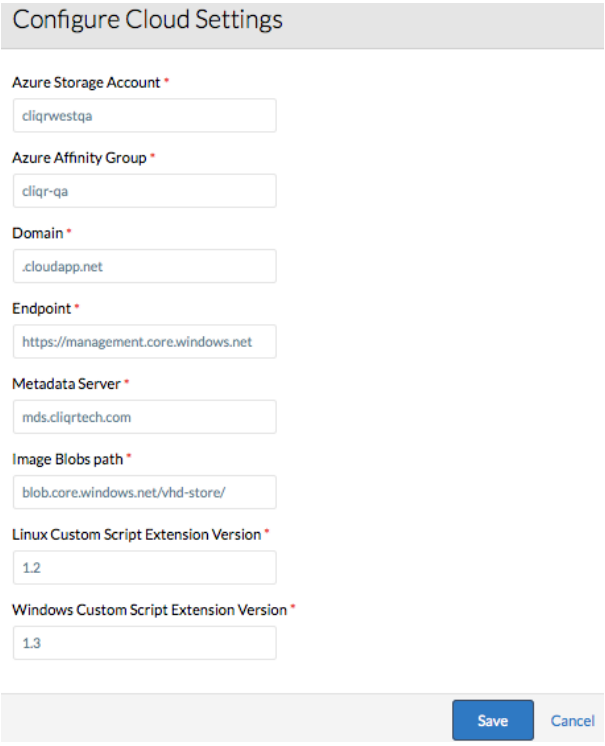


4. [リージョン（Region）] タブをクリックし、クラウド リージョンを追加します。
   a. [クラウド リージョンの追加（Add Cloud Region）] をクリックします。
   b. このクラウドに必要なリージョンを選択します。
   c. このクラウド リージョンの [リージョン名（Region Name）] およびオプションの [表示名（Display Name）] を追加します。
   d. [保存（Save）] をクリックします。

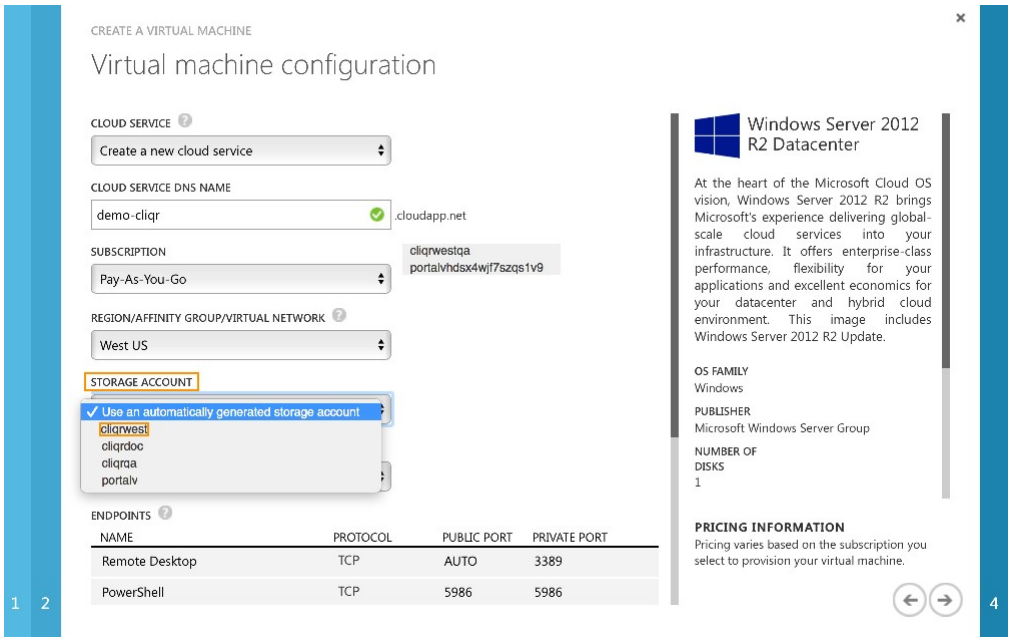
> インスタンス タイプ、ストレージ タイプ、およびイメージ マップのセクションは、リージョンを追加するとすぐに自動的に設定されます。

5. [クラウド設定の編集（Edit Cloud Settings）] リンクをクリックして、このクラウド リージョンに必要な設定を更新し、[保存（Save）] をクリックします。

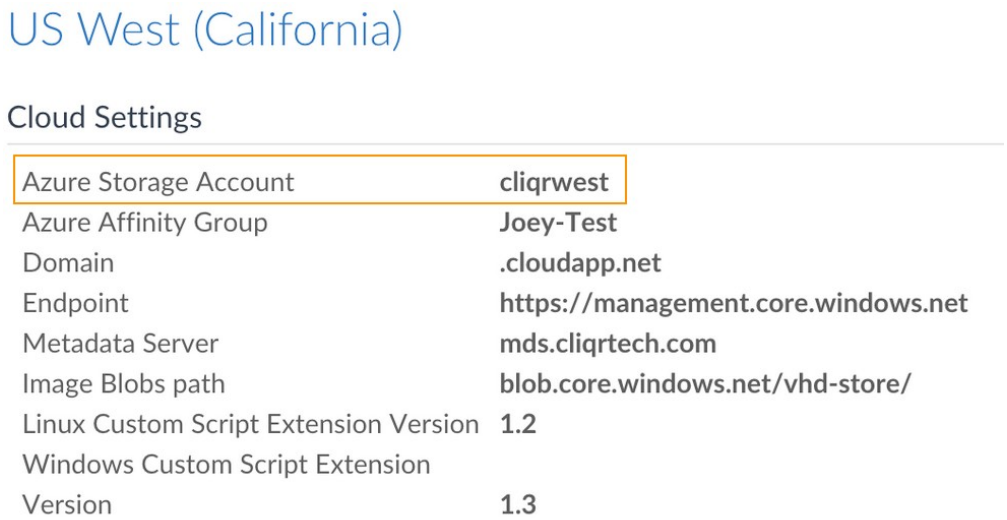
> **注意**
> **クラウド設定を編集**する場合、変更を CCO に保存し、これらの変更がファイアウォールの設定内の CCO にも反映されるようにする必要があります。
>
> CCO がすでに設定されている場合は、これらのクラウド設定を有効にするために CCO を再登録する必要があります。

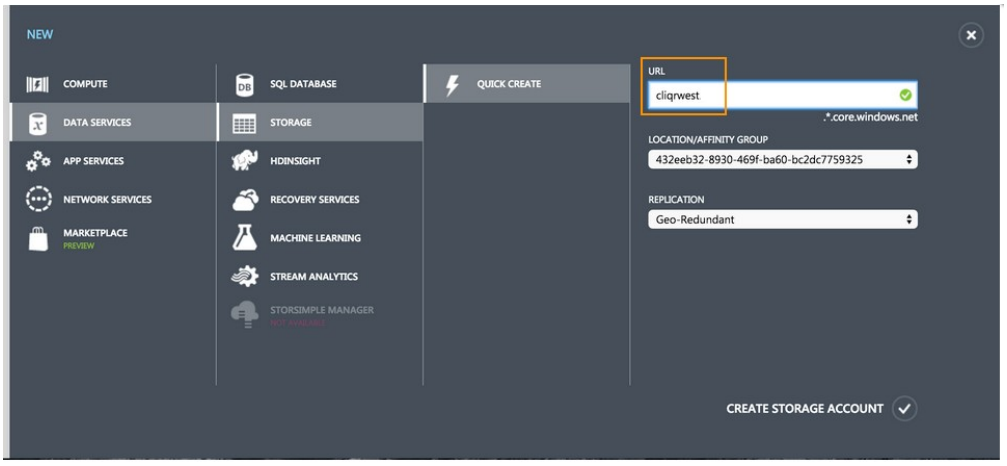


- Azure ストレージ アカウント（Azure Storage Account）：次の Azure、および対応する CloudCenter のイメージの例で示すように、このフィールドには、対応する Azure アカウント（URL フィールド）をセットアップする際に使用された名前と同じ名前が含まれている必要があります。**Azure の設定例**を以下に示します。



対応する CloudCenter の設定例:





> 既存のストレージ アカウントを使用する場合は、**Azure Classic ポータル**の [STORAGE] タブで必要な値を見つけることができます。既存のストレージ アカウントの正確な名前で検索し、このアカウントが CCO と同じクラウド リージョンにあることを確認します。

- Azure アフィニティ グループ(Azure Affinity Group):新しいアフィニティ グループを作成するか、既存のアフィニティ グループを使用することができます。

> 既存のアフィニティ グループを使用する場合は、**Azure Classic ポータル**の [SETTINGS] タブで必要な値を見つけることができます。既存のアフィニティ グループの正確な名前で検索し、このグループが CCO と同じクラウド リージョンにあることを確認します。

- Azure ネットワーク（Azure Network）：このネットワークにわかりやすい名前を付けます。この値には、どのような文字列も入力できます。
- ドメイン（Domain）：パブリック IP でインスタンスを起動すると、Azure はドメインの DNS 名を作成することを許可します。このフィールドに表示されるデフォルト値は .cloud.app.net です。CloudCenter プラットフォームで作成したホスト サービス名をこの値の前に付ける必要があります。設定した Azure ドメインが .cloud.app.net ではない場合、デフォルト値を適切に変更し、その値の前に有効なホスト サービス名を付けます。

> 既存のドメインを使用する場合は、**Azure Classic ポータル**の [CLOUD SERVICES] タブで必要な値を見つけることができます。必要なクラウド サービスにアクセスし、[Dashboard] をクリックして、DNS 名を検索します。

- エンドポイント（Endpoint）：コールの宛先の API エンドポイント。このコールを行うために使用される CloudCenter REST API の URL。ほとんどの場合（営利目的の設定、中国を除く設定の場合）、この値をそのまま使用できます。この値は、新しい政府リージョンや中国内のリージョンに必要な変更に対応するよう設定できます。
- メタデータ サーバ（Metadata Server）：このフィールドは、ノードに関する追加情報（CCO IP アドレス、その他の詳細）を提供します。このフィールドは、主にブートストラッピングのために使用します。企業は、アプリケーション VM と CCO にアウトバウンド インターネット アクセスがあることを確認する必要があります。または、企業は、この通信を行うためのサーバを社内に設定できます。
- イメージ BLOB パス（Image Blobs path）：Microsoft Storage のアカウント名（OS ドライブおよびデータ ディスクドライブの情報が保存されている場所）。このフィールドには、デフォルトで、デフォルトの URL が表示されます。URL がこのフィールドに表示されるデフォルト URL と異なる場合は、URL を blob.core.windows.net/<Azure_Storage_Account_name> に更新してください。ほとんどの場合（営利目的の設定、中国を除く設定の場合）、この値をそのまま使用できます。この値は、新しい政府リージョンや中国内のリージョンに必要な変更に対応するよう設定できます。
- Linux カスタム スクリプト拡張機能のバージョン（Linux Custom Script Extension Version）：エージェントのないノードで自動ブートストラップを実行するために CloudCenter プラットフォームにより使用される Microsoft Azure プラグイン バージョン（追加情報については、「Custom Windows Image」を参照）。ほとんどの場合（営利目的の設定、中国を除く設定の場合）、この値をそのまま使用できます。この値は、新しい政府リージョンや中国内のリージョンに必要な変更に対応するよう設定できます。
- Windows カスタム スクリプト拡張機能のバージョン（Windows Custom Script Extension Version）：エージェントのないノードで自動ブートストラップを実行するために CloudCenter プラットフォームにより使用される Microsoft Windows プラグイン バージョン（追加情報については、「Custom Windows Image」を参照）。ほとんどの場合（営利目的の設定、中国を除く設定の場合）、この値をそのまま使用できます。この値は、新しい政府リージョンや中国内のリージョンに必要な変更に対応するよう設定できます。

6. クラウド設定を完了するには、CCO を CCM に登録する必要があります。
   CCM への CCO の登録

CCM への CCO の登録

- クラウド リージョンの微妙な違い
- 非 HA モード
- HA モード

クラウド リージョンの微妙な違い

CCM に CCO を登録すると、CCO は登録されたクラウド リージョンにのみ動作します。

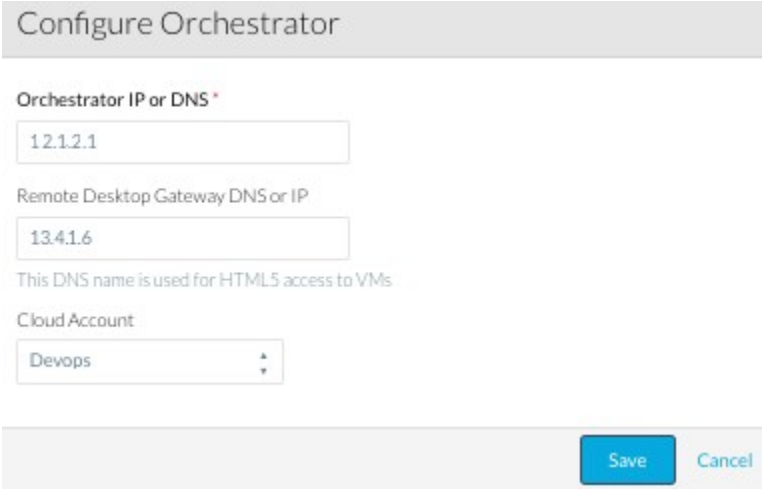
> **CloudCenter**
> CCM に CCO を登録すると、CloudCenter プラットフォームは、このクラウド リージョンがアクティブであると見なし、特定条件下でしか CloudCenter プラットフォームからこのクラウド リージョンを削除できなくなります。詳細については、「Cloud Region Configuration」>「*Delete Cloud Region*」を参照してください。

> 提供された例では AWS クラウドを参照していますが、スクリーン キャプチャはクラウドごとに異なることがある点に注意してください。

非 HA モード

CCM に CCO を登録するには、次の手順に従います。

a. [オーケストレータの設定（Configure Orchestrator）] ポップアップで、CCM からアクセス可能な CCO の IP アドレスを入力し、CCO をホストするために使用されるクラウド アカウントを選択します。



b. このページがまだ表示されていない場合は、必要なクラウドにおいて、[管理(Admin)] > [クラウド(Clouds)] > [リージョンの設定(Configure Regions)] を選択していることを確認します。
   i. [リージョン(Regions)] タブの [オーケストレータの設定(Configure Orchestrator)] をクリックします。
   ii. オーケストレータの IP または DNS(Orchestrator IP or DNS):CCO サーバの IP または DNS アドレスを指定します。
   iii. リモート デスクトップ ゲートウェイの DNS または IP(Remote Desktop Gateway DNS or IP):Guacamole サーバの IP アドレス(VM へのブラウザベースのアクセスを有効化)。Guacamole コンポーネントが AMQP サーバ内に存在している場合は、AMQP サーバの IP アドレスを指定します。
   iv. クラウド アカウント(Cloud Account):この CCO で使用するクラウド アカウントを選択します。

> **Amazon クラウドの微妙な違い**
> IAM ロールを設定している場合、この設定は重要です。必ずこのロールを含むクラウド アカウントを選択してください。

c. [保存(Save)] をクリックします。これで、CCM と CCO の相互信頼関係が確立されました。CloudCenter プラットフォームは現在、導入された CCO によりクラウド リージョンを管理しています。
d. 手順 2 と手順 3 を繰り返し、CCM とその他の CCO 間の相互信頼を確立します。

CCO VM を登録し、設定が完了しました。ここでは、2 つのオプションがあります。

- その他のクラウド リージョンを追加し、これらのクラウドごとに CCO を登録します。詳細については、「クラウド リージョンごと(必須)」を参照してください。
- イメージをマッピングします。詳細については、「イメージ マッピング」を参照してください。

> クラウド アカウントのイメージを起動するアクセス許可を付与する必要がある場合は、「Image Launch Permissions」を参照してください。

- アプリケーションのモデリング、展開、および管理を行います。詳細については、「Application Profile」を参照してください。

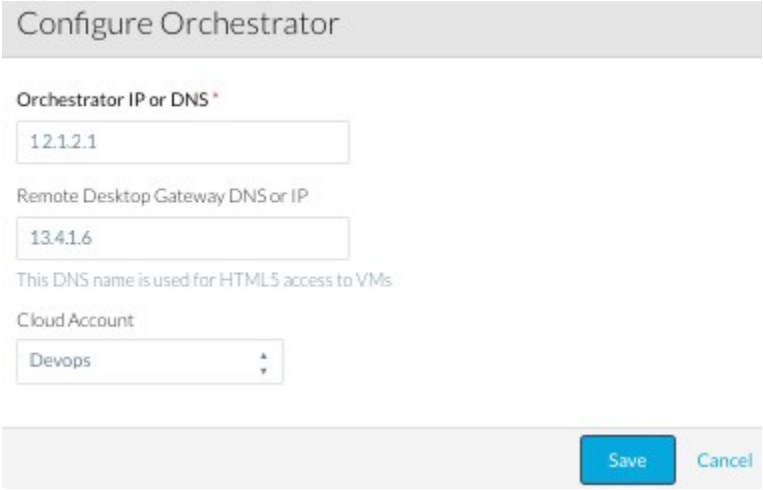
HA モード

CCM に CCO を登録するには、次の手順に従います。

a. プライマリ CCO で Tomcat Service が実行中であることを確認します。
b. セカンダリ CCO およびターシャリ CCO にログインし、両方のサーバで Tomcat Service を停止します。

```
/etc/init.d/tomcat stop
```

c. CCM UI にアクセスし、CCO LB の IP アドレスを使用して CCO を登録します。
   i. このページがまだ表示されていない場合は、必要なクラウドにおいて、[管理(Admin)] > [クラウド(Clouds)] > [リージョンの設定(Configure Regions)] を選択していることを確認します。
   ii. [リージョン(Regions)] タブの [オーケストレータの設定(Configure Orchestrator)] をクリックします。
   iii. CCM からアクセス可能な CCO の IP アドレスを入力し、CCO をホストするために使用されるクラウド アカウントを選択します。



1. オーケストレータの IP または DNS（Orchestrator IP or DNS）：CCO サーバの IP または DNS アドレスを指定します。
2. リモート デスクトップ ゲートウェイの DNS または IP（Remote Desktop Gateway DNS or IP）：Guacamole サーバの IP アドレス（VM へのブラウザベースのアクセスを有効化）。Guacamole コンポーネントが AMQP サーバ内に存在している場合は、AMQP サーバの IP アドレスを指定します。
3. クラウド アカウント（Cloud Account）：この CCO で使用するクラウド アカウントを選択します。必ずこのロールを含むクラウド アカウントを選択してください。
4. [保存（Save）] をクリックします。これで、CCM と CCO の相互信頼関係が確立されました。CloudCenter プラットフォームは現在、導入された CCO によりクラウド リージョンを管理しています。

d. 登録が成功したら、プライマリ CCO サーバにログインします。
e. プライマリ CCO の **/usr/local/osmosix/etc/** フォルダから、セカンダリ CCO およびターシャリ CCO の両サーバ上の**同じ場所**に **gateway_config.properties** ファイルをコピーします。
f. すべてのサーバのコピーしたファイルの所有権およびアクセス許可が次のようになっていることを確認します。
   - オーナー（Owner）= cliqruser
   - グループ権限（Group Permission）= 読み取りおよび書き込み
g. 必要な場合は、次のコマンドを実行して設定を変更します。

```
chown
cliqruser:cliqruser
/usr/local/osmosix/etc/gateway_config.properties
chmod 644 /usr/local/osmosix/etc/gateway_config.properties
```

h. 各サーバで次のコマンドを発行することによって、セカンダリ CCO とターシャリ CCO サーバで Tomcat を起動します。

```
/etc/init.d/tomcat start
```

i. HA モードのその他の CCO についてこの手順を繰り返し、CCM とその他の CCO 間の相互信頼を確立します。

CCO VM を登録し、設定が完了しました。ここでは、2 つのオプションがあります。

- その他のクラウド リージョンを追加し、これらのクラウドごとに CCO を登録します。詳細については、「クラウド リージョンごと（必須）」を参照してください。
- イメージをマッピングします。詳細については、「イメージ マッピング」を参照してください。

> クラウド アカウントのイメージを起動するアクセス許可を付与する必要がある場合は、「Image Launch Permissions」を参照してください。

- アプリケーションのモデリング、展開、および管理を行います。詳細については、「Application Profile」を参照してください。

戻る：クラウドの設定

- Alibaba クラウドの設定

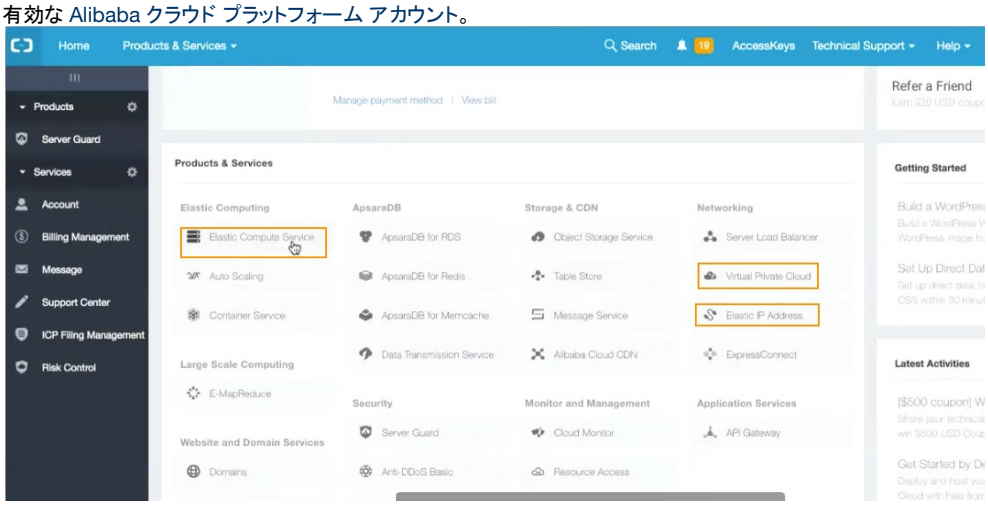
Alibaba クラウドの設定

> 次のスクリーン キャプチャは、Alibaba クラウド プラットフォームが変更されると変わる可能性があることに注意してください。この項ではあくまでも参考として示しています。

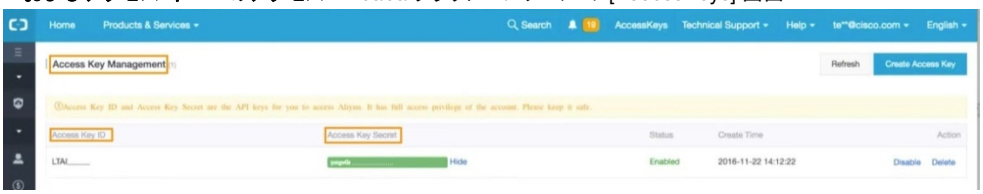
前提条件

CloudCenter プラットフォームで Alibaba クラウドをマッピングする前に、次の Alibaba 要件を確認します。

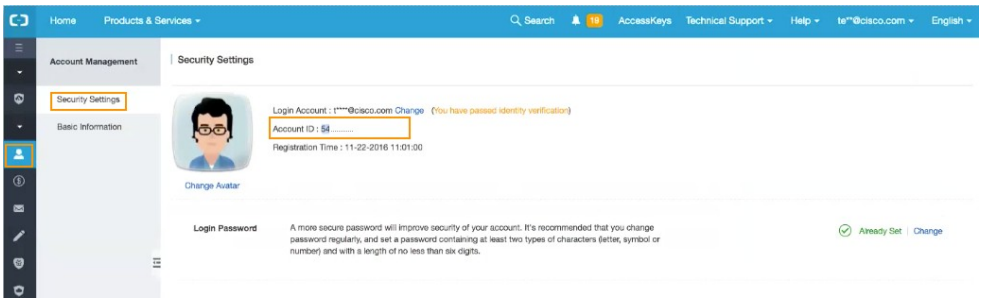
- 有効な Alibaba クラウド プラットフォーム アカウント。



- 以下のサービスへのアクセス（上の画像のオレンジ色の四角形で強調表示されていて、Alibaba クラウド コンソールでこれらのサービスを有効にする必要があります）。
  - **Elastic コンピューティング サービス**
  - **仮想プライベート クラウド**
  - **Elastic IP アドレス**
- **ID およびアクセス キーへのアクセス**：Alibaba クラウド コンソールの [AccessKeys] 画面：



  - **アクセス ID**：Alibaba クラウド アクセス キー ID は Alibaba クラウド API へのアクセスの ID 証明です。
  - **アクセス キー**：このアカウントのアクセス パラメータを識別するための 28 文字の Alibaba クラウド アクセス キー シークレット。
- **アカウント ID**：Alibaba クラウド コンソールの [Security Settings] 画面：この設定は、アカウントをリンクし、イメージをダウンロードするために必要です。

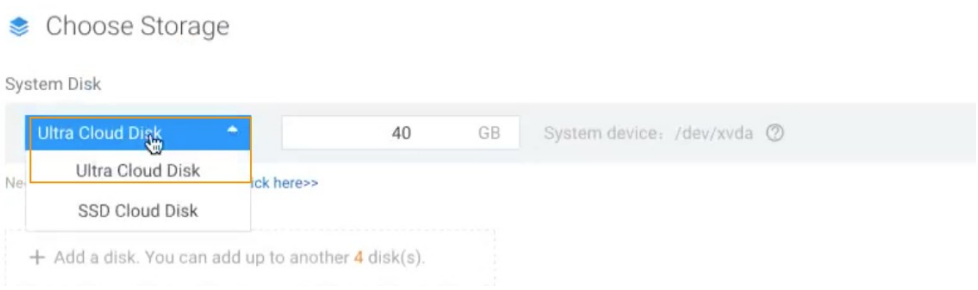


制限事項

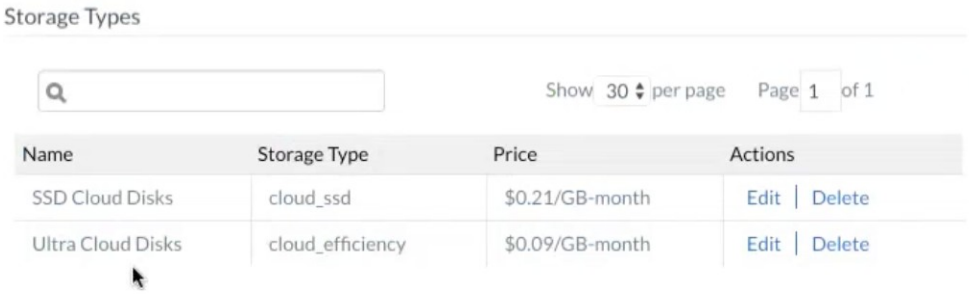
Alibaba クラウドを設定するときは、次の制限事項に注意してください。

- 各リージョンでサポートされるインスタンスはリージョンによって異なります。Alibaba SDK と Alibaba Web インターフェイスでは、各ゾーンにリストされるインスタンスが異なります。CCM UI を使用して新しいインスタンスを追加できます。詳細については、「インスタンス タイプの管理」を参照してください。
- Alibaba クラウドでは、現在、カスタム イメージ上のユーザ データの照会/設定は許可されていません。
  - CloudCenter プラットフォームは、各インスタンスのユーザ データを取得するのに、シスコからホストされるメタデータ サービス（mds.cliqrtech.com）に依存します。これには、パブリック IP アドレスが必要です。
  - 管理者が Alibaba のパブリック イメージを使用する場合、CloudCenter プラットフォームは Alibaba のメタデータ サービスを使用してこれらのイメージを取得します。

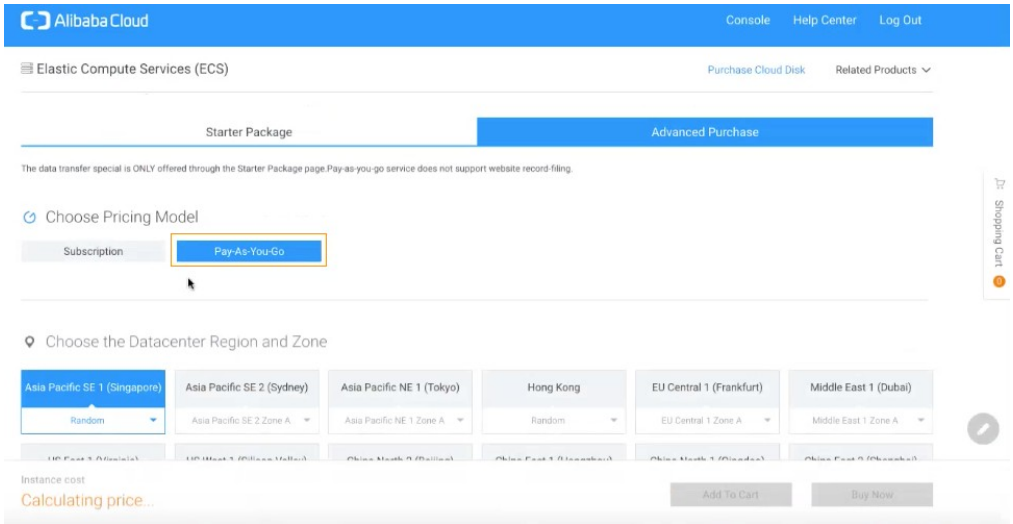
- CloudCenter プラットフォームは、現在、OS（システム ディスク）の Ultra クラウド ディスク - クラウド効率化ディスク構成をサポートします（これは Alibaba クラウドのデフォルト設定です）。SSD クラウド ディスク オプションは現在、システム ディスクでは CloudCenter プラットフォームでサポートされません。



ただし、データ ディスクのストレージ タイプを展開するときは、CloudCenter プラットフォームは両方のオプションをサポートします。

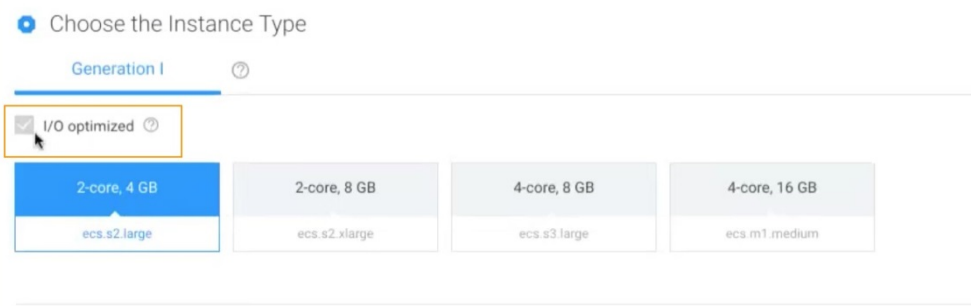


- CloudCenter プラットフォームは、Elastic IP アドレスを使用してのみ、パブリック IP をサポートします。このため、ユーザは 0 Mbps の帯域幅を選択できます。Elastic IP プールを作成するとき、管理者は、アプリケーションの要件に従ってアカウントに最大帯域幅を割り当てることができます。Alibaba コンソールで必要なゾーンを選択し、環境の必要に応じてこの設定を構成します。
- 任意のリージョンの Alibaba クラウドでリソースが不足すると、*完売*（または API の場合、リソースが不足している）としてマークされます。CloudCenter ユーザは Alibaba のコンソールをチェックし、リソースが利用可能になると操作を再試行します。
- すべてのインスタンスは**従量制**モデルで価格設定されています。CloudCenter プラットフォームでは、Alibaba のサブスクリプションベースの価格設定モデルがサポートされていません。

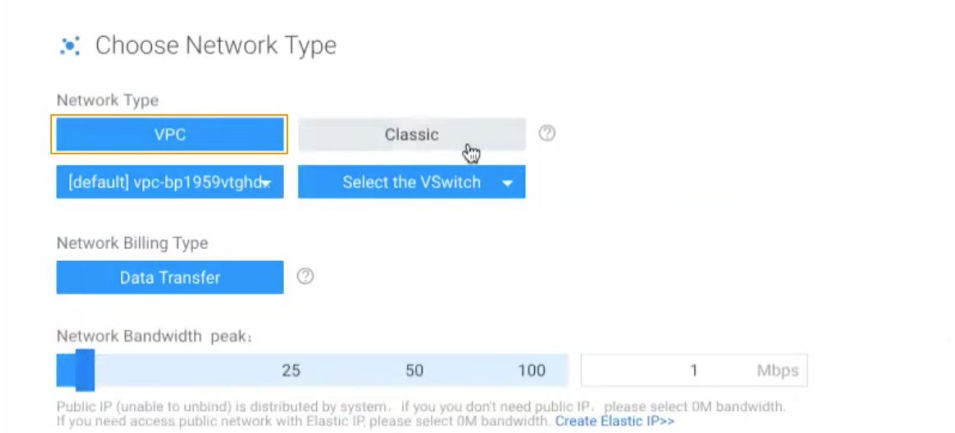


インスタンスの課金タイプは常に従量制モデルに基づいて**ポストペイド**されます。

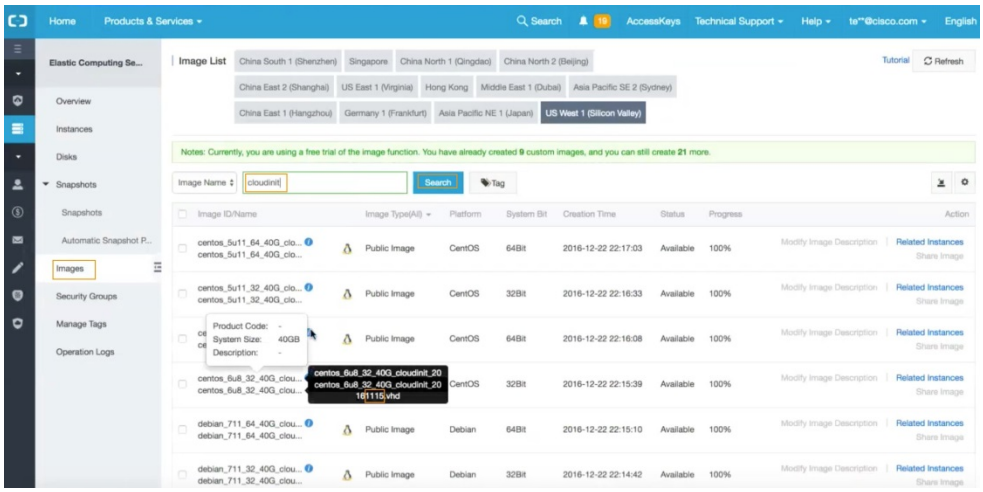
- CloudCenter プラットフォームでは、すべてのインスタンスの **I/O が最適化されている**と見なします（ほとんどの設定のデフォルトであり、設定できません）。



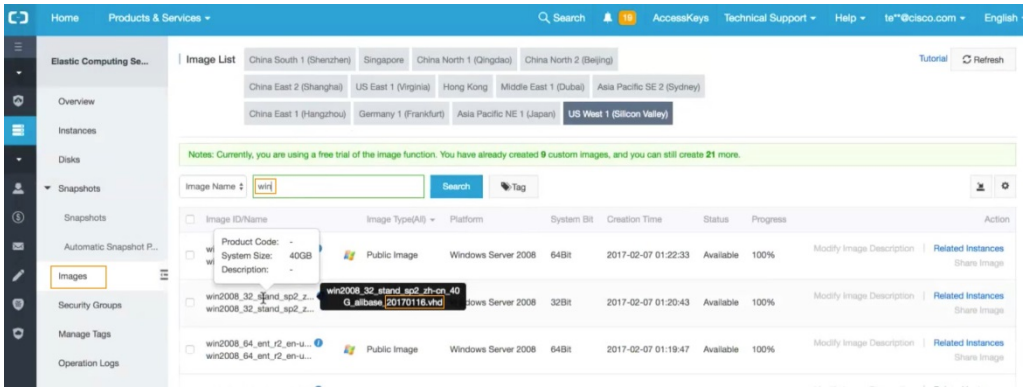
- CloudCenter プラットフォームは Alibaba のクラシック ネットワーク タイプをサポートしておらず、VPC ネットワーク タイプのみをサポートしています。



- CloudCenter プラットフォームは、次のような末尾のイメージ名のみをサポートしています。
  - Linux **cloudinit** イメージ：末尾が **20160728**、**20161115** 以降である必要があります。



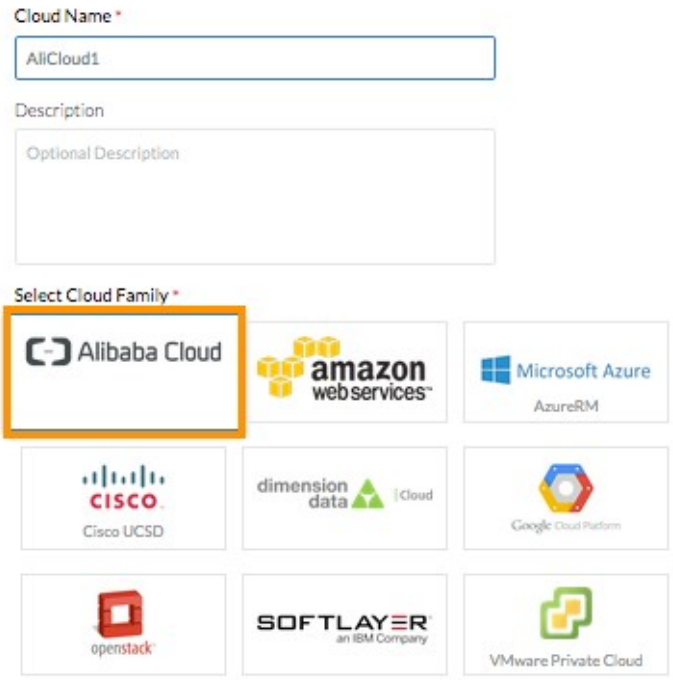
  - Windows win イメージ：末尾が **20160622** 以降である必要があります。



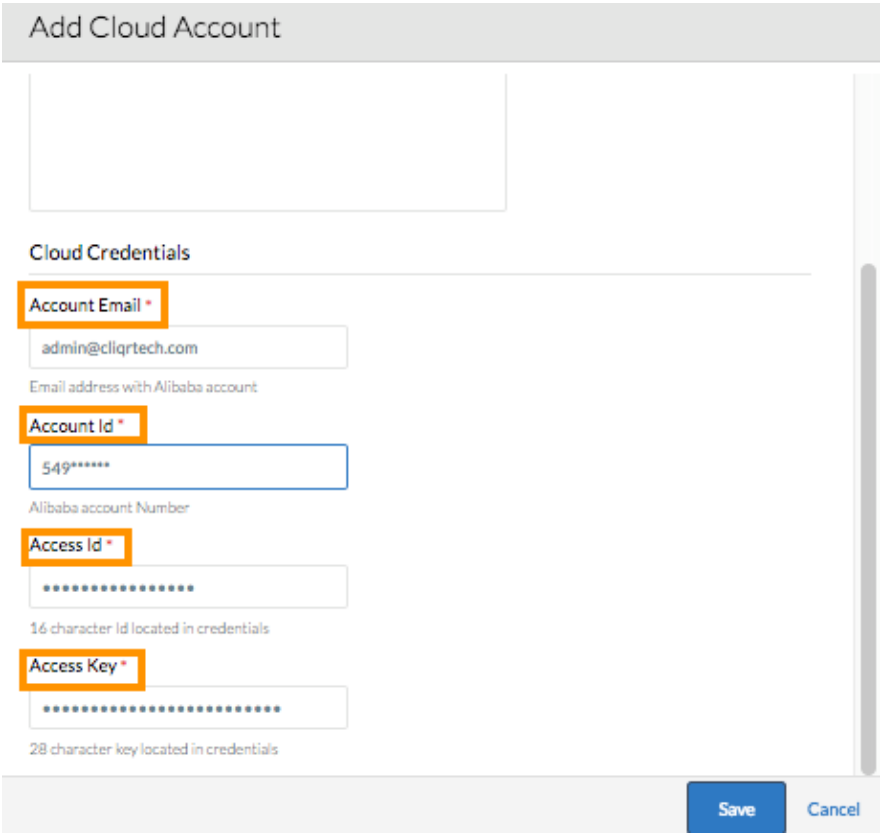
設定プロセス

Alibaba クラウドで論理マッピングを設定するには、次の手順に従います。

1. CCM UI にアクセスし、CCM UI のメインメニューで [管理（Admin）] > [クラウド（Clouds）] > [クラウドの追加（Add Cloud）] を選択します。

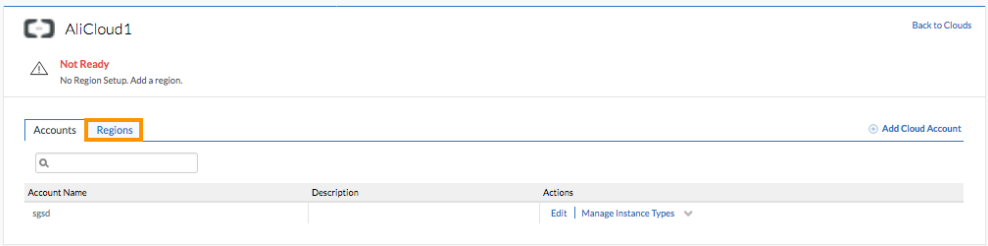


2. [Alibaba Cloud Platform] オプションを選択し、このクラウドの名前と説明を入力して、[保存(Save)] をクリックします。
3. 新たに追加されたクラウドを見つけて [クラウド アカウントの追加(Add Cloud Account)] リンクをクリックします。[クラウド アカウントの追加(Add Cloud Account)] ポップアップが表示されます。



   a. 新しいクラウドに名前を割り当てます。
   b. Alibaba アカウントに関連付けられている次のクラウド クレデンシャルを追加し、[保存(Save)] をクリックします。
      i. アカウントの電子メール(Account Email):Alibaba クラウド プラットフォーム アカウントへのログインに使用した電子メールアドレス。
      ii. アカウント ID(Account Id):上記の「*前提条件*」セクションで指定されている、Alibaba アカウントの Alibaba アカウント ID。
      iii. アクセス ID(Access Id):上記の「*前提条件*」セクションで指定されている Alibaba アカウントの 16 文字の Alibaba アクセス キー ID。
      iv. アクセス キー(Access Key):上記の「*前提条件*」セクションで指定されている Alibaba アカウントの 28 文字の API アクセス シークレット。

4. [リージョン（Regions）] タブをクリックします。



5. [リージョン（Region）] タブをクリックし、クラウド リージョンを追加します。
   a. [クラウド リージョンの追加（Add Cloud Region）] をクリックします。
   b. このクラウドに必要なリージョンを選択します。
   c. このクラウド リージョンの [リージョン名（Region Name）] およびオプションの [表示名（Display Name）] を追加します。
   d. [保存（Save）] をクリックします。

> インスタンス タイプ、ストレージ タイプ、およびイメージ マップのセクションは、リージョンを追加するとすぐに自動的に設定されます。

6. （任意）[クラウド設定の編集（Edit Cloud Settings）] をクリックし、各リージョンの Alibaba クラウド設定を更新します。
   - リージョン エンドポイント（Region Endpoint）：選択したリージョン名が自動的に入力されます。
   - **[インスタンスの命名方法（Instance Naming Strategy）]** と **[インスタンス IPAM の使用（Instance IPAM Strategy）]**：これらの値の設定の詳細については、「VM Name Config」セクションを参照してください。

> **注意**
> **クラウド設定を編集**する場合、変更を CCO に保存し、これらの変更がファイアウォールの設定内の CCO にも反映されるようにする必要があります。
>
> CCO がすでに設定されている場合は、これらのクラウド設定を有効にするために CCO を再登録する必要があります。

7. クラウド設定を完了するには、CCO を CCM に登録する必要があります。
   CCM への CCO の登録

CCM への CCO の登録

- クラウド リージョンの微妙な違い
- 非 HA モード
- HA モード

クラウド リージョンの微妙な違い

CCM に CCO を登録すると、CCO は登録されたクラウド リージョンにのみ動作します。

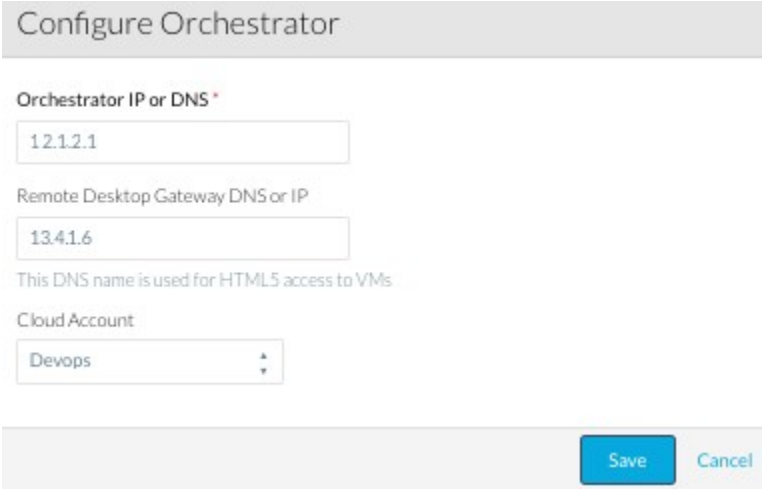
> **CloudCenter**
> CCM に CCO を登録すると、CloudCenter プラットフォームは、このクラウド リージョンがアクティブであると見なし、特定条件下でしか CloudCenter プラットフォームからこのクラウド リージョンを削除できなくなります。詳細については、「Cloud Region Configuration」>「*Delete Cloud Region*」を参照してください。

> 提供された例では AWS クラウドを参照していますが、スクリーン キャプチャはクラウドごとに異なることがある点に注意してください。

非 HA モード

CCM に CCO を登録するには、次の手順に従います。

a. [オーケストレータの設定（Configure Orchestrator）] ポップアップで、CCM からアクセス可能な CCO の IP アドレスを入力し、CCO をホストするために使用されるクラウド アカウントを選択します。



b. このページがまだ表示されていない場合は、必要なクラウドにおいて、[管理(Admin)] > [クラウド(Clouds)] > [リージョンの設定(Configure Regions)] を選択していることを確認します。
   i. [リージョン(Regions)] タブの [オーケストレータの設定(Configure Orchestrator)] をクリックします。
   ii. オーケストレータの IP または DNS(Orchestrator IP or DNS):CCO サーバの IP または DNS アドレスを指定します。
   iii. リモート デスクトップ ゲートウェイの DNS または IP(Remote Desktop Gateway DNS or IP):Guacamole サーバの IP アドレス(VM へのブラウザベースのアクセスを有効化)。Guacamole コンポーネントが AMQP サーバ内に存在している場合は、AMQP サーバの IP アドレスを指定します。
   iv. クラウド アカウント(Cloud Account):この CCO で使用するクラウド アカウントを選択します。

> **Amazon クラウドの微妙な違い**
> IAM ロールを設定している場合、この設定は重要です。必ずこのロールを含むクラウド アカウントを選択してください。

c. [保存(Save)] をクリックします。これで、CCM と CCO の相互信頼関係が確立されました。CloudCenter プラットフォームは現在、導入された CCO によりクラウド リージョンを管理しています。
d. 手順 2 と手順 3 を繰り返し、CCM とその他の CCO 間の相互信頼を確立します。

CCO VM を登録し、設定が完了しました。ここでは、2 つのオプションがあります。

- その他のクラウド リージョンを追加し、これらのクラウドごとに CCO を登録します。詳細については、「クラウド リージョンごと(必須)」を参照してください。
- イメージをマッピングします。詳細については、「イメージ マッピング」を参照してください。

> クラウド アカウントのイメージを起動するアクセス許可を付与する必要がある場合は、「Image Launch Permissions」を参照してください。

- アプリケーションのモデリング、展開、および管理を行います。詳細については、「Application Profile」を参照してください。

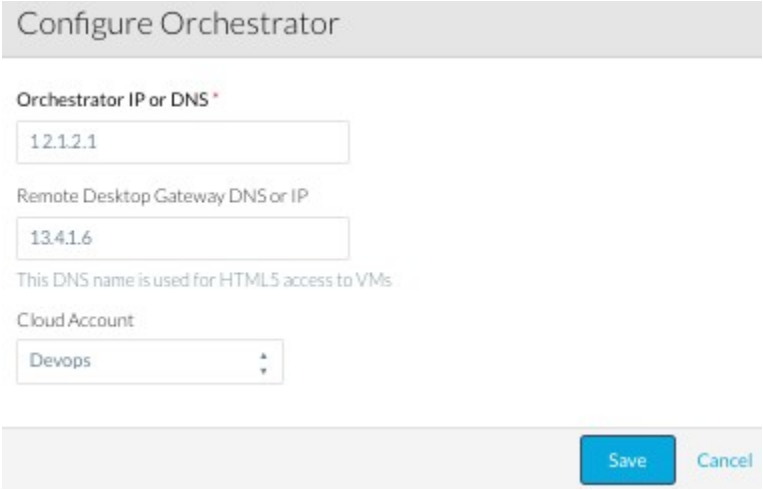
HA モード

CCM に CCO を登録するには、次の手順に従います。

a. プライマリ CCO で Tomcat Service が実行中であることを確認します。
b. セカンダリ CCO およびターシャリ CCO にログインし、両方のサーバで Tomcat Service を停止します。

```
/etc/init.d/tomcat stop
```

c. CCM UI にアクセスし、CCO LB の IP アドレスを使用して CCO を登録します。
   i. このページがまだ表示されていない場合は、必要なクラウドにおいて、[管理(Admin)] > [クラウド(Clouds)] > [リージョンの設定(Configure Regions)] を選択していることを確認します。
   ii. [リージョン(Regions)] タブの [オーケストレータの設定(Configure Orchestrator)] をクリックします。
   iii. CCM からアクセス可能な CCO の IP アドレスを入力し、CCO をホストするために使用されるクラウド アカウントを選択します。



1. オーケストレータの IP または DNS（Orchestrator IP or DNS）：CCO サーバの IP または DNS アドレスを指定します。
2. リモート デスクトップ ゲートウェイの DNS または IP（Remote Desktop Gateway DNS or IP）：Guacamole サーバの IP アドレス（VM へのブラウザベースのアクセスを有効化）。Guacamole コンポーネントが AMQP サーバ内に存在している場合は、AMQP サーバの IP アドレスを指定します。
3. クラウド アカウント（Cloud Account）：この CCO で使用するクラウド アカウントを選択します。必ずこのロールを含むクラウド アカウントを選択してください。
4. [保存（Save）] をクリックします。これで、CCM と CCO の相互信頼関係が確立されました。CloudCenter プラットフォームは現在、導入された CCO によりクラウド リージョンを管理しています。

d. 登録が成功したら、プライマリ CCO サーバにログインします。
e. プライマリ CCO の **/usr/local/osmosix/etc/** フォルダから、セカンダリ CCO およびターシャリ CCO の両サーバ上の**同じ場所**に **gateway_config.properties** ファイルをコピーします。
f. すべてのサーバのコピーしたファイルの所有権およびアクセス許可が次のようになっていることを確認します。
   - オーナー（Owner）= cliqruser
   - グループ権限（Group Permission）= 読み取りおよび書き込み
g. 必要な場合は、次のコマンドを実行して設定を変更します。

```
chown
cliqruser:cliqruser
/usr/local/osmosix/etc/gateway_config.properties
chmod 644 /usr/local/osmosix/etc/gateway_config.properties
```

h. 各サーバで次のコマンドを発行することによって、セカンダリ CCO とターシャリ CCO サーバで Tomcat を起動します。

```
/etc/init.d/tomcat start
```

i. HA モードのその他の CCO についてこの手順を繰り返し、CCM とその他の CCO 間の相互信頼を確立します。

CCO VM を登録し、設定が完了しました。ここでは、2 つのオプションがあります。

- その他のクラウド リージョンを追加し、これらのクラウドごとに CCO を登録します。詳細については、「クラウド リージョンごと（必須）」を参照してください。
- イメージをマッピングします。詳細については、「イメージ マッピング」を参照してください。

> クラウド アカウントのイメージを起動するアクセス許可を付与する必要がある場合は、「Image Launch Permissions」を参照してください。

- アプリケーションのモデリング、展開、および管理を行います。詳細については、「Application Profile」を参照してください。

戻る：クラウドの設定

注意
[クラウド リージョン(Cloud Region)] ページ([CCM UI] > [管理(Admin)] >[クラウド(Clouds)] > [リージョンの設定(Configure Region)])の [クラウド設定の編集(Edit Cloud Settings)] で設定を編集したら、[オーケストレータの設定(Configure Orchestrator)]、次に [保存(Save)] をクリックして、変更内容を CCO に保存し、これらの変更がファイアウォール設定内の CCO にもプロパゲートされていることを確認する必要があります。

CCM への CCO の登録

- クラウド リージョンの微妙な違い
- 非 HA モード
- HA モード

クラウド リージョンの微妙な違い

CCM に CCO を登録すると、CCO は登録されたクラウド リージョンにのみ動作します。

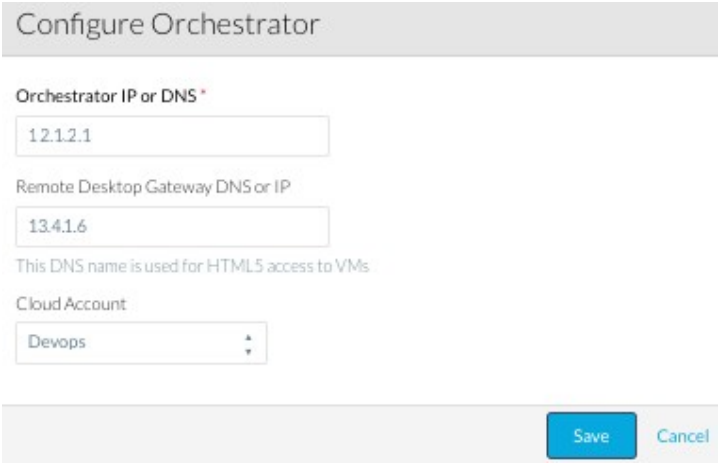
CloudCenter
CCM に CCO を登録すると、CloudCenter プラットフォームは、このクラウド リージョンがアクティブであると見なし、特定条件下でしか CloudCenter プラットフォームからこのクラウド リージョンを削除できなくなります。詳細については、「Cloud Region Configuration」>「*Delete Cloud Region*」を参照してください。

提供された例では AWS クラウドを参照していますが、スクリーン キャプチャはクラウドごとに異なることがある点に注意してください。

非 HA モード

CCM に CCO を登録するには、次の手順に従います。

1. [オーケストレータの設定(Configure Orchestrator)] ポップアップで、CCM からアクセス可能な CCO の IP アドレスを入力し、CCO をホストするために使用されるクラウド アカウントを選択します。



2. このページがまだ表示されていない場合は、必要なクラウドにおいて、[管理(Admin)] > [クラウド(Clouds)] > [リージョンの設定(Configure Regions)] を選択していることを確認します。
   a. [リージョン(Regions)] タブの [オーケストレータの設定(Configure Orchestrator)] をクリックします。
   b. オーケストレータの IP または DNS(Orchestrator IP or DNS):CCO サーバの IP または DNS アドレスを指定します。
   c. リモート デスクトップ ゲートウェイの DNS または IP(Remote Desktop Gateway DNS or IP):Guacamole サーバの IP アドレス(VM へのブラウザベースのアクセスを有効化)。Guacamole コンポーネントが AMQP サーバ内に存在している場合は、AMQP サーバの IP アドレスを指定します。
   d. クラウド アカウント(Cloud Account):この CCO で使用するクラウド アカウントを選択します。

   Amazon クラウドの微妙な違い
   IAM ロールを設定している場合、この設定は重要です。必ずこのロールを含むクラウド アカウントを選択してください。

3. [保存(Save)] をクリックします。これで、CCM と CCO の相互信頼関係が確立されました。CloudCenter プラットフォームは現在、導入された CCO によりクラウド リージョンを管理しています。
4. 手順 2 と手順 3 を繰り返し、CCM とその他の CCO 間の相互信頼を確立します。

CCO VM を登録し、設定が完了しました。ここでは、2 つのオプションがあります。

- その他のクラウド リージョンを追加し、これらのクラウドごとに CCO を登録します。詳細については、「クラウド リージョンごと(必須)」を参照してください。
- イメージをマッピングします。詳細については、「イメージ マッピング」を参照してください。

> クラウド アカウントのイメージを起動するアクセス許可を付与する必要がある場合は、「Image Launch Permissions」を参照してください。

- アプリケーションのモデリング、展開、および管理を行います。詳細については、「Application Profile」を参照してください。

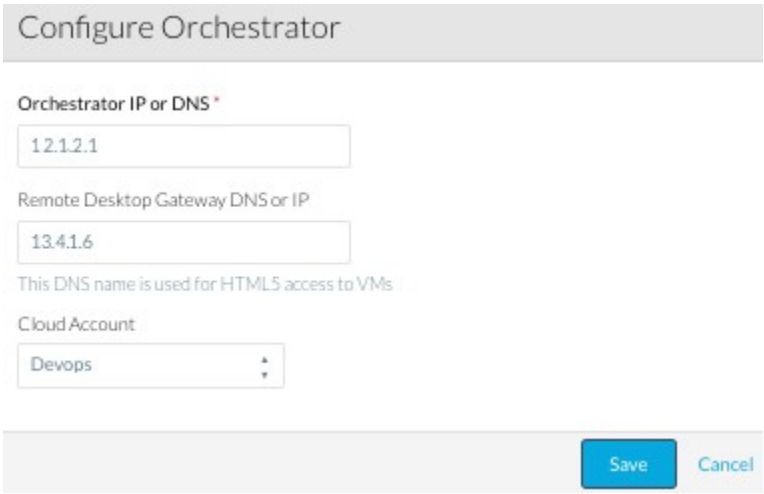
HA モード

CCM に CCO を登録するには、次の手順に従います。

1. プライマリ CCO で Tomcat Service が実行中であることを確認します。
2. セカンダリ CCO およびターシャリ CCO にログインし、両方のサーバで Tomcat Service を停止します。

```
/etc/init.d/tomcat stop
```

3. CCM UI にアクセスし、CCO LB の IP アドレスを使用して CCO を登録します。
   a. このページがまだ表示されていない場合は、必要なクラウドにおいて、[管理(Admin)] > [クラウド(Clouds)] > [リージョンの設定(Configure Regions)] を選択していることを確認します。
   b. [リージョン(Regions)] タブの [オーケストレータの設定(Configure Orchestrator)] をクリックします。
   c. CCM からアクセス可能な CCO の IP アドレスを入力し、CCO をホストするために使用されるクラウド アカウントを選択します。



      i. オーケストレータの IP または DNS(Orchestrator IP or DNS):CCO サーバの IP または DNS アドレスを指定します。
      ii. リモート デスクトップ ゲートウェイの DNS または IP(Remote Desktop Gateway DNS or IP):Guacamole サーバの IP アドレス(VM へのブラウザベースのアクセスを有効化)。Guacamole コンポーネントが AMQP サーバ内に存在している場合は、AMQP サーバの IP アドレスを指定します。
      iii. クラウド アカウント(Cloud Account):この CCO で使用するクラウド アカウントを選択します。必ずこのロールを含むクラウド アカウントを選択してください。
      iv. [保存(Save)] をクリックします。これで、CCM と CCO の相互信頼関係が確立されました。CloudCenter プラットフォームは現在、導入された CCO によりクラウド リージョンを管理しています。
4. 登録が成功したら、プライマリ CCO サーバにログインします。
5. プライマリ CCO の **/usr/local/osmosix/etc/** フォルダから、セカンダリ CCO およびターシャリ CCO の両サーバ上の**同じ場所**に **gateway_config.properties** ファイルをコピーします。
6. すべてのサーバのコピーしたファイルの所有権およびアクセス許可が次のようになっていることを確認します。
   - オーナー(Owner)= cliqruser
   - グループ権限(Group Permission)= 読み取りおよび書き込み
7. 必要な場合は、次のコマンドを実行して設定を変更します。

```
chown
cliqruser:cliqruser
/usr/local/osmosix/etc/gateway_config.properties chmod 644
/usr/local/osmosix/etc/gateway_config.properties
```

8. 各サーバで次のコマンドを発行することによって、セカンダリ CCO とターシャリ CCO サーバで Tomcat を起動します。

```
/etc/init.d/tomcat start
```

9. HA モードのその他の CCO についてこの手順を繰り返し、CCM とその他の CCO 間の相互信頼を確立します。

CCO VM を登録し、設定が完了しました。ここでは、2 つのオプションがあります。

- その他のクラウド リージョンを追加し、これらのクラウドごとに CCO を登録します。詳細については、「クラウド リージョンごと（必須）」を参照してください。
- イメージをマッピングします。詳細については、「イメージ マッピング」を参照してください。

> クラウド アカウントのイメージを起動するアクセス許可を付与する必要がある場合は、「Image Launch Permissions」を参照してください。

- アプリケーションのモデリング、展開、および管理を行います。詳細については、「Application Profile」を参照してください。

イメージ マッピング

- 概要
- [クラウド構成（Cloud Configurations）] タブでの方法
- [イメージ（Images）] タブでの方法
- サービス マッピングの変更
- イメージ マッピングの同期
- インスタンス タイプ
- ルート ディスク サイズ

概要

アプリケーション VM イメージをインストールした後は、CloudCenter VA ベース イメージのイメージ ID を、このクラウド リージョンでの CloudCenter の論理イメージ名にマッピングします。

クラウド間でイメージ ID が異なるため、イメージ マッピングもクラウドに基づいて異なります。詳細については、「イメージ ID の設定」の項を参照してください。

CloudCenter VA ベース イメージ ID を CloudCenter の論理イメージ名にマッピングするには、[クラウド構成（Cloud Configurations）] タブでの方法、または [イメージ（Images）] タブでの方法を使用できます。

> シスコでは、データセンターとプライベート クラウド用のアウトオブボックス イメージ マッピングを提供していません。アプリケーション VM のイメージ マッピングを設定すると、利用可能なサービスが表示されます。

[クラウド構成（Cloud Configurations）] タブでの方法

CloudCenter VA ベース イメージ ID を CloudCenter プラットフォームの論理イメージ名にマッピングするには、次の手順に従います。

1. CCM UI のメインメニューに表示される [管理（Admin）] リンクをクリックします。
2. サイド パネルで [クラウド構成（Cloud Configurations）] リンクをクリックし、[クラウド構成（Cloud Configurations）] ページを表示します。
3. 必要なクラウドに対し [設定（Configure）] リンク（[アクション（Actions）] 列）をクリックします。
4. [クラウド リージョン（Cloud Regions）] セクションまでスクロールし、必要なリージョンに対し [設定（Configure）] リンクをクリックします。
5. [イメージ マッピングの設定（Configure Image Mappings）] セクションまでスクロールし、必要な CloudCenter ベース OS イメージについて [マッピングの追加（Add Mapping）] をクリックします。
   次に例を示します。
   - CentOS 7
   - RHEL 7
   - Ubuntu12.04

Configure Image Mappings

Image Name	Description	Mapping	Actions
CentOS 5.x	CentOS 5.x	N/A	Add Mapping
CentOS 6.2 with IBM Services	CentOS 6.2 with IBM Services	N/A	Add Mapping
CentOS 6.2 with WSO2 Services	CentOS 6.2 with WSO2 Services	N/A	Add Mapping
CentOS 6.x	CentOS 6.x	N/A	Add Mapping
External Service RDS	External Service RDS	N/A	Add Mapping
RHEL 5.x	RHEL 5.x	N/A	Add Mapping
RHEL 5.x Oracle Services	RHEL 5.x Oracle Services	N/A	Add Mapping
Shared Storage	Shared Storage	N/A	Add Mapping
SLES11 with SAP Hana	SLES11 with SAP Hana	N/A	Add Mapping
SUSE Linux Enterprise 11	SUSE Linux Enterprise 11	N/A	Add Mapping
Ubuntu 10.10	Ubuntu 10.10	N/A	Add Mapping
Ubuntu 12.04	Ubuntu 12.04	N/A	Add Mapping
Ubuntu 12.04 with Webapp Services	Ubuntu 12.04 with Webapp Services	N/A	Add Mapping
Windows Server 2008 R2 SP1	Windows Server 2008 R2 SP1	N/A	Add Mapping
Windows Server 2008 R2 SP1 with Windows Services	Windows Server 2008 R2 SP1 with Windows Services	N/A	Add Mapping
Windows Server 2012	Windows Server 2012	N/A	Add Mapping
Windows Server 2012 with MSSQL Service	Windows Server 2012 with MSSQL Service	N/A	Add Mapping

a. [インスタンス タイプの追加（Add Instance Type）] をクリックして新しいインスタンス タイプ（「インスタンス タイプの管理」を参照）マッピングを追加するか、既存のマッピングを上書きします。
b. [保存（Save）] をクリックし、新しく追加されたインスタンス タイプを保存します。
c. 導入の必要に応じて、他のイメージに対してこのプロセスを繰り返します。

[イメージ（Images）] タブでの方法

「Manage Cloud Mapping」を参照してください。

サービス マッピングの変更

デフォルトでは、[サービス（Services）] タブ内のすべてのサービスが、CentOS 6 または RHEL 6 イメージにマッピングされます。

> **コメント**
> CloudCenter の導入で他のイメージを使用する場合は、CCM UI で適用可能なイメージを明示的に指定する必要があります。

サービス変更をマッピングするには、次の手順に従います。

1. CCM UI のメインメニューの [管理（Admin）] リンクをクリックします。
2. [サービス（Services）] リンクをクリックします。
3. [編集（Edit）] をクリックし、導入に適用可能なサービスを編集します。
4. [サービスの編集（Edit Service）] ページで、[サポートするイメージ（Supporting Images）] フィールドの設定を確認します。
5. 選択内容を、使用中の環境で使用するイメージに変更します。
6. [保存（Save）] をクリックします。

イメージ マッピングの同期

> この手順を実行するには、パッケージ ストアにアクセスできる必要があります。

パッケージ ストアのクラウド イメージ マッピングに同期することができます。この機能により、管理者は、クラウド プロバイダーのイメージ マッピング定義に変更が見つかったときに情報を同期することができます。一度に 1 つのクラウド リージョン（1 つのクラウドに属するすべてのクラウド リージョンでなく）の情報のみ同期できます。

イメージ マッピングを同期するには、次の手順に従います。

1. 「クラウドの設定」ページで指定したとおりにクラウド リージョンを設定します。
2. CCM への CCO の登録。
3. [CCO（オーケストレータ）設定（CCO (Orchestrator) Configuration）] セクションに [実行中（Running）] ステータスが表示されたら、[イメージ マッピングの同期（Sync Image Mappings）] をクリックします。
4. [クラウド リージョン（Cloud Regions）] ページが更新されて、同期されたステータスが表示されます。

インスタンス タイプ

詳細については、「インスタンス タイプの管理」を参照してください。

ルート ディスク サイズ

詳細については、「インスタンス タイプの管理」>「*ルート ディスク サイズ*」を参照してください。

インスタンス タイプの管理

- 概要
- インスタンス タイプの例
- インスタンス タイプの追加
- インスタンス タイプの同期
- 課金管理
- スクラッチ ディスク ストレージ（ローカル ストレージ）
- ルート ディスク サイズ
- インスタンス タイプの非表示

概要

CloudCenter は、イメージ マップ プロセス中に管理者によって選択されたアプリケーション VM インスタンス タイプのみを表示します。

- CloudCenter は、イメージ マップ プロセス中に提供されたインスタンスだけを自動的にリストするよう、[インスタンス タイプ（Instance Type）] ドロップダウンをフィルタリングします。
- 選択したクラウドにイメージ マッピングがない場合や、イメージと選択したクラウドとに互換性がない場合、CloudCenter はインスタンス タイプを表示しません。
- インスタンス タイプは、パブリック クラウドでは動的に設定されます。導入のためにインスタンス タイプを追加すると、[インスタンス タイプの設定（Configure Instance Types）] セクションに設定済みのインスタンスが表示されるようになります。
- 管理者は、マッピングされたイメージを編集して、追加のインスタンス タイプをサポートできます。
- クラウド リージョンにインスタンス タイプを追加すると、ユーザはローカル ストレージとしてゼロ ディスク サイズを指定できます。0（ゼロ）の場合は、イメージ内のディスクが使用され、追加のディスクは VM に導入されません。
- インスタンス タイプおよびイメージの同期へのサポートは、AWS SoftLayer、Azure、AzureRM、Google、および Dimension Data で提供されます。

インスタンス タイプの例

企業用のインスタンス タイプを入力します。CloudCenter プラットフォームで定義されているサンプル インスタンス タイプを次に示します。

Instance Type	Name	Hardware Spec	Cost Per Hour	Actions
small	small	2CPUs, 2048GB, 1000Mbps	0.2	Edit | Delete
medium	medium	2CPUs, 4096GB, 1000Mbps	0.3	Edit | Delete
large	large	4CPUs, 8192GB, 1000Mbps	0.6	Edit | Delete
xlarge	xlarge	4CPUs, 16384GB, 1000Mbps	1.2	Edit | Delete
2xlarge	2xlarge	8CPUs, 32768GB, 1000Mbps	2.4	Edit | Delete

インスタンス タイプの追加

インスタンス タイプを追加するには、次の手順に従います。

1. CCM UI のメインメニューに表示される [管理（Admin）] リンクをクリックします。
2. サイド パネルで [クラウド構成（Cloud Configurations）] リンクをクリックし、[クラウド構成（Cloud Configurations）] ページを表示します。
3. 必要なクラウドに対し [設定（Configure）] リンク（[アクション（Actions）] 列）をクリックします。
4. [クラウド リージョン（Cloud Regions）] セクションまでスクロールし、必要なリージョンに対し [設定（Configure）] リンクをクリックします。
5. [イメージ マッピングの設定（Configure Image Mappings）] セクションまでスクロールし、必要なイメージについて [マッピングの追加（Add Mapping）] をクリックします。
6. [インスタンス タイプの追加（Add Instance Type）] をクリックして新しいインスタンス タイプ マッピングを追加するか、既存のマッピングを上書きします。
7. [保存（Save）] をクリックし、新しく追加されたインスタンス タイプを保存します。
8. 導入の必要に応じて、他のイメージに対してこのプロセスを繰り返します。

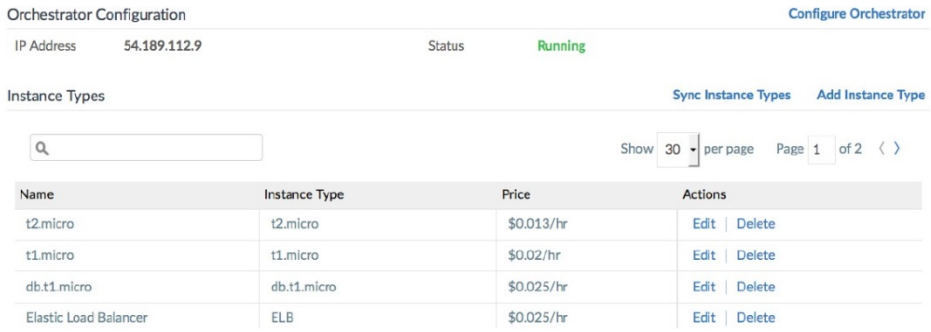
インスタンス タイプの同期

⚠ この手順を実行するには、パッケージ ストアにアクセスできる必要があります。

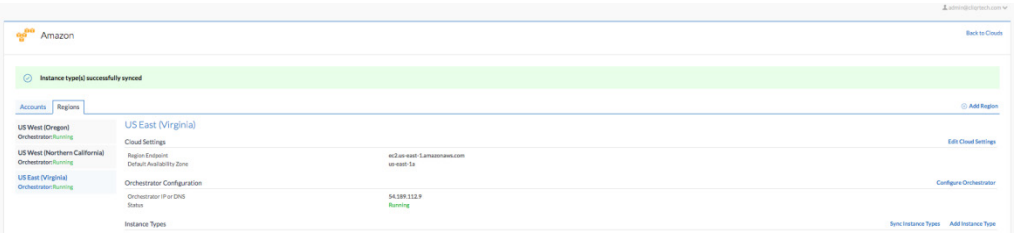
管理者は、パッケージ ストアからインスタンス タイプおよび価格情報を同期できます。この機能により、管理者は、クラウド プロバイダーのインスタンス タイプ定義および価格情報に変更を見つけたときに、情報を同期できます（他の課金情報については、「Tenant Billing」を参照してください）。

インスタンス タイプを同期するには、次の手順に従います。

1. 「クラウドの設定」ページで指定したとおりにクラウド リージョンを設定します。
2. CCM への CCO の登録。
3. [CCO（オーケストレータ）設定（CCO (Orchestrator) Configuration）] セクションに [実行中（Running）] ステータスが表示されたら、[インスタンス タイプの同期（Sync Instance Types）] をクリックします。



4. [クラウド リージョン（Cloud Regions）] ページが更新されて、同期されたステータスが表示されます。



課金管理

ユーザへの課金の追加情報については、「Tenant Billing」>「*Granular Billing Control*」を参照してください。

スクラッチ ディスク ストレージ（ローカル ストレージ）

通常、ルート ディスクはクラウド イメージによって制御され、CloudCenter プラットフォームによりサイズ変更されません。ほとんどのクラウドには自動化されたサイズ変更オプションはありません。アプリケーション VM のルート ディスクは導入に使用されるイメージと必ず同じサイズです。

CloudCenter プラットフォームでは、クラウド イメージ ルート ディスクのサイズに関係なく、インスタンス タイプの追加的（2 次的）サイズが提供されます。このサイズは、エクストラ ストレージ用に VM に追加されている追加のディスク（インストール ベースの OS イメージ）用です。

> このローカル ストレージは、イメージ テンプレートにあるドライブに加えて、2 番目のハード ドライブとして追加されます。

導入時に CloudCenter プラットフォームから VM に割り当てられる追加ディスク サイズには独自の要件があります。ユーザが、インスタンス タイプによってサポートされるディスク ボリューム サイズを超えて追加した場合、導入は失敗し、関連付けられているクラウドから対応するエラー メッセージが発行されます。

インスタンス タイプ定義中のストレージ サイズ設定は、ユーザがインスタンス タイプを選択する際にどのようなハードウェア仕様を採用するかを理解するための（単に表示目的の）ものです。AWS や Azure などのパブリック クラウドでは、インスタンス タイプとそのハードウェア仕様はすべてクラウドによって事前定義されます。この設定を 2000 GB に変更しても、2000 GB の一時的ディスクが作成されるわけではありません。

ルート ディスク サイズ

ルート ディスク サイズの動作は、次の表に示すクラウドに依存します。

クラウド	クラウドごとのイメージ ディスク サイズの特徴
AWS	インスタンス タイプ ディスク サイズは一時的（一時的スクラッチ）ディスク用のサイズであり、ルート ディスク サイズは VM イメージで指定されるサイズです。一部のインスタンス タイプは複数の一時的ディスクを含む場合があります。

Azure	動作は AWS と類似しています。インスタンス タイプ ディスク サイズは一時的ディスク用で、ルート ディスク サイズは VM イメージで指定されるサイズです。インスタンス タイプによって、最大ルート ディスクのサイズに制限があります。 Azure インスタンス タイプのストレージ サイズは、一時的な(temp)ディスク サイズを意味します。A4\ExtraLarge を選択した場合、一時的ディスクは 650 GB になります。
OpenStack	インスタンス タイプ ディスク サイズはルート ディスク サイズ用です。インスタンス タイプが 40 GB のディスクを指定し、ベース イメージは 20 GB のルート ディスク サイズの場合、このイメージとインスタンス タイプを使用して VM が起動すると、ルート ディスクは自動的に 40 GB にサイズ変更します。ただし、ベース イメージが 80 GB のルート ディスクで、ユーザが 40 GB のディスク サイズを指定するものと同じインスタンス タイプを選択した場合、VM の起動は失敗します。
VMware	VMware にはインスタンス タイプの概念はありません。CloudCenter プラットフォームの定義では、インスタンス タイプ ディスク サイズは一時的ディスク用です。インスタンス タイプでディスク サイズが指定されている場合、このインスタンス タイプを使用する VM が起動するとき、CloudCenter プラットフォームは、指定のサイズの別のディスクを VM にアタッチします。追加情報については、「VMware Configurations」>「Resize VM Root Disk」を参照してください。

インスタンス タイプの非表示

⚠ インスタンス タイプは、各リージョンに固有のものではありません。インスタンスによっては一部のリージョンで使用できません。注意してください。

指定した ベース OS イメージの [インスタンス タイプ(Instance Type)] ドロップダウンに使用可能なインスタンス タイプが表示されない場合、次の設定を確認してください。

- ベース イメージ マッピング:イメージをマッピングするときに、次の情報を確認してください(「イメージ マッピング」を参照)。
  - サービスが必要なベース OS イメージを使用していること、およびイメージ マッピングが定義済みであること。
  - (クラウド マッピングを追加するか、またはクラウド マッピングを編集する際に)イメージのインスタンス タイプを選択するとき、必要なインスタンス タイプがマッピングされていることを確認してください。
- ハードウェア仕様:使用する仕様が、ターゲットの インスタンス タイプの設定よりも低いことを確認します。上記の「インスタンス タイプの例」の項に挙げたいくつかの例を参照してください。
- インスタンス タイプのアーキテクチャ設定:32 ビットおよび 64 ビット アーキテクチャのサポートを確認するため、[両方(Both)] オプションの選択を試行してから、導入を再実行します。

クラウド ストレージの設定

- 概要
- クラウドのサポート
- クラウド ストレージ タイプ
- クラウド ストレージの追加
- ストレージ タイプの同期
- ストレージ課金

概要

CloudCenter プラットフォームでは、ジョブの課金プロセス内のコンピューティング コストとストレージ コストを考慮することができます。CloudCenter プラットフォームは、割り当てられたストレージ量と、IOPS のようなストレージのプロパティに基づいてクラウド ストレージの課金を計算します。

ⓘ 現在、CloudCenter プラットフォームでは、ストレージ デバイス間でのデータ転送に基づいてクラウド ストレージの課金を計算する機能はありません。

ストレージまたはボリュームの情報は、複数のボリューム オブジェクトを使用して計算されます。VolumeInfoSet には、volumeInfo オブジェクト(type (volumeInfos)およびその他の関連プロパティを持つ)とインスタンス ID のリストがあります。volumeInfoSet は、ジョブのアプリケーション設定に JSON 文字列として格納されます。課金時にストレージ コストを計算するには、VolumeInfoSet 設定を使用する必要があります。

クラウドのサポート

クラウド環境	サポート対象?	注記(Notes)
• OpenStack • VMware	○	課金を考慮するには、クラウド ストレージ タイプとそのコストを定義します。
• AWS • Google	○	課金は、課金を考慮するように割り当てられたボリュームに基づきます。
その他すべてのクラウド	なし	コストはボリュームの使用状況に基づいてアカウンティングされ、使用状況のアカウンティングはできません

クラウド ストレージ タイプ

クラウド ストレージ タイプ（cloudStorageType）は、CCM からクラウド ストレージ関連情報を取得するために使用される新しいタイプです。このタイプを使用すると、プライベート クラウドでは独自のストレージ タイプをモデル化し、パブリック クラウドでは既存のクラウド ストレージ タイプをキャプチャすることができます。

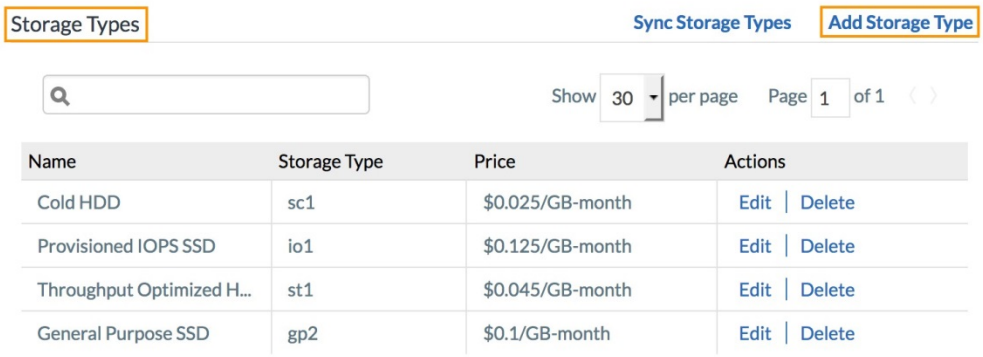
クラウド ストレージ タイプ	説明
SSD	ソリッド ステート ドライブ：永続的にデータを格納するメモリとして集積回路アセンブリを使用するストレージ デバイス タイプ。
HDD	ハード ディスク ドライブ：磁性材料を使用して永続的にデータを格納するストレージ デバイス タイプ。
ホットとコールド	アクセス頻度データ。 • ホット：頻繁にアクセスされるデータ • コールド：アクセス頻度の低いデータ
IOPS	入出力操作毎秒：1 秒あたりに実行された読み取りまたは書き込み操作の量。SSD、HDD などのコンピュータ ストレージ デバイスの特性評価に使用されるパフォーマンス測定。
IO サイズ	オペレーティング システムと、ディスクへのアクセスを必要とするアプリケーション/サービスに依存し、同時に一定量のデータの読み取り/書き込み要求を発行します。たとえば、4 KB、8 KB、32 KB などです。
スループット（Throughput）	特定のファイル サイズで一定期間内に転送されたメガバイト数の平均値の測定。*スループット（MB/秒）= 平均 IO サイズ x IOPS*

クラウド ストレージの追加

課金は、クラウド ストレージ タイプの価格情報に基づいて行われます。CCM サーバの初期化時にクラウド ストレージ タイプを設定することもできます。

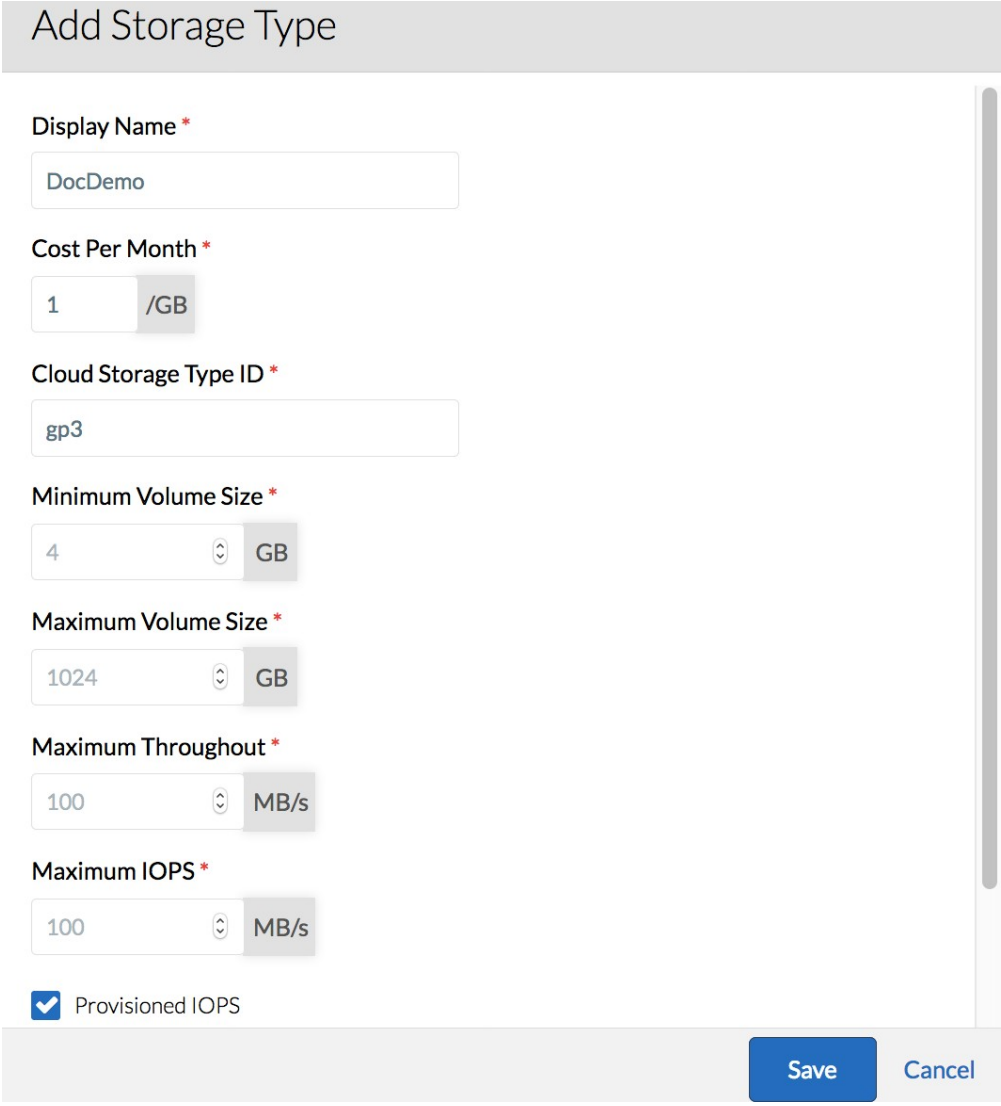
クラウド ストレージを設定するには、次の手順に従います。

1. CCM UI から [管理（Admin）] > [クラウド（Clouds）] > *クラウド名*をクリックします。右側に、このクラウドに設定されているリージョンのリストが表示されます。
2. [リージョンの追加（Add Region）] をクリックして、クラウド リージョンを追加します。[リージョンの追加（Add Region）] ポップアップが表示されます。
3. このクラウド リージョンの [リージョン名（Region Name）] およびオプションの [表示名（Display Name）] を追加します。
4. [ストレージ タイプ（Storage Types）] セクションまで下にスクロールします。



5. [ストレージ タイプの追加（Add Storage Type）] をクリックし、新しいストレージ タイプのマッピングを追加します。[ストレージ タイプの追加（Add Storage Type）] ポップアップが表示されます。

> ⚠ [クラウド ストレージの追加（Add Cloud Storage）] オプションは、OpenStack と VMware のクラウドでのみ使用できます。管理者ユーザは、設定されたリージョンに必要なストレージ タイプを明示的に含めるか、**ストレージ タイプの同期**オプションが必要なクラウド ストレージ タイプをインポートするようにする必要があります。
>
> [クラウド ストレージの追加（Add Cloud Storage）] フィールドはパブリック クラウドでは利用できません。設定されたストレージ オプションは**編集**できますが、パブリック クラウドの [表示名（Display Name）] 以外のフィールドのデータは編集されません。



6. ストレージ設定に基づいてフィールドを設定します。詳細については、上記の「クラウド ストレージ タイプ」の表を参照してください。
7. [保存(Save)] をクリックします。

ストレージ タイプの同期

管理者は、パッケージ ストアからストレージ タイプおよび価格情報を同期できます。この機能により、管理者は、クラウド プロバイダーのストレージ タイプ定義および価格情報に変更を見つけたときに、情報を同期できます(他の課金情報については、「Tenant Billing」を参照してください)。

> ストレージ タイプは、リモート リポジトリに存在する必要があります。
>
> この手順を実行するには、パッケージ ストアにアクセスできる必要があります。

ストレージ タイプを同期するには、次の手順に従います。

1. 「クラウドの設定」ページで指定したとおりにクラウド リージョンを設定します。
2. CCM への CCO の登録。
3. [CCO(オーケストレータ)設定(CCO (Orchestrator) Configuration)] セクションに [実行中(Running)] ステータスが表示されたら、[ストレージ タイプの同期(Sync Storage Types)] をクリックします。
4. [クラウド リージョン(Cloud Regions)] ページが更新されて、同期されたステータスが表示されます。

ストレージ課金

ストレージ課金を考慮するには、ストレージ コストを考慮するためにインスタンス タイプを定義するのと同様に、(ユーザが)ストレージ タイプを定義する必要があります。

導入時にインスタンス タイプを選択すると、ハードウェア仕様情報を使用してインスタンスが起動します。同じように、ボリューム情報が導入におけるストレージ課金に使用されます。

ストレージ タイプにはコスト情報とその他のストレージ関連のプロパティ(スループットなど)が含まれるため、CloudCenter プラットフォームはこのストレージ サイズおよびタイプを使用して課金を計算します。

- パブリック クラウドの場合、定義されているストレージ タイプはクラウドで定義されたストレージ タイプと一致する必要があるため、CloudCenter はストレージのコストを考慮することができます。
- プライベート クラウドの場合:
  - ストレージ タイプはユーザ定義です(クラウドで定義されていません)。
  - ジョブの展開時にユーザ定義のストレージ タイプで指定されたボリューム情報がストレージ コストの計算に使用されます。
  - VMware(および他のプライベート クラウド)では、ストレージ タイプは課金目的でのみ使用され、展開目的では使用されません。
  - ジョブの展開目的では、volumeInfos > *size* 入力が使用されます。

課金の追加情報については、「Tenant Billing」>「*Granular Billing Control*」を参照してください。

イメージ ID の設定

- 概要
- イメージ ID のクラウドごとの特徴
- ベース OS イメージをダウンロードおよびインポートして、イメージ ID を取得します

概要

CloudCenter プラットフォームは、CCM および CCO アプライアンスに加え、Ubuntu12.04、Ubuntu14.04、CentOS6、および Ubuntu Web アプライアンス用のベース OS イメージをサポートします。CloudCenter がサポートするイメージを使用するか、選択したインポート アプライアンスを使用するかを選択できます(追加情報については、「Image Administration」を参照)。いずれにしても、アプライアンスをダウンロードし、各アプライアンスに対し、イメージ ID を取得する必要があります。イメージ ID は、イメージ マッピングをする際に、クラウドでアプライアンスを参照するために必要です。

イメージ ID のクラウドごとの特徴

イメージ ID の用語は、クラウド間で異なります。

- VMware のイメージ ID

  <VM name >/ <snapshot name>

  スナップショットを使用する場合は、vSphere にフォルダを追加し(CloudCenter のスナップショットを保存するため)、***CliqrTemplates*** という名前を付けて、このスナップショット ***CliqrTemplates*** フォルダに追加します。

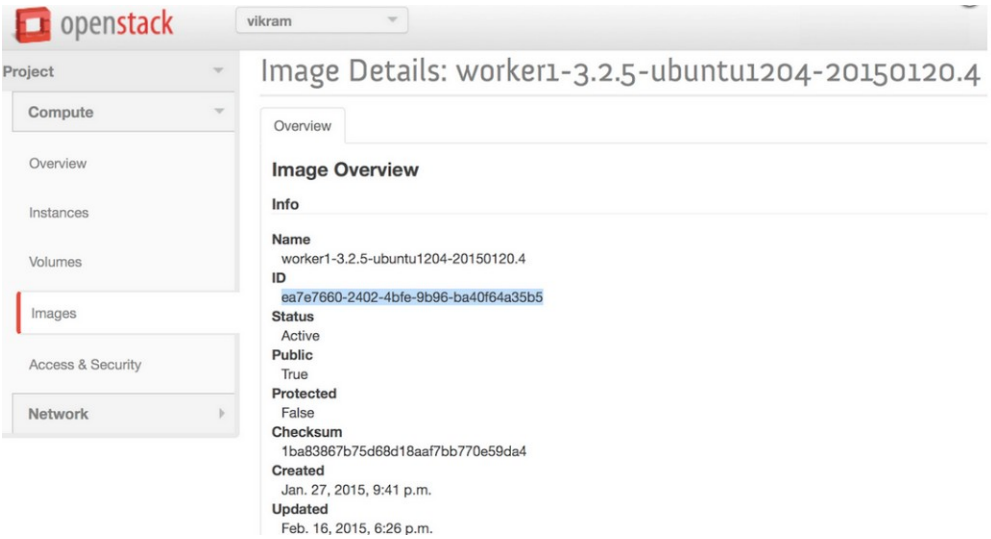
  または、VM テンプレート名を使用してクラウド イメージを設定することもできます。この場合、VMware コンソールおよびシステム上のイメージ ID は常に指定されたデータストアまたはデータストア クラスタに対して完全な複製を実行するため、VM または VM テンプレートの名前を指定します。

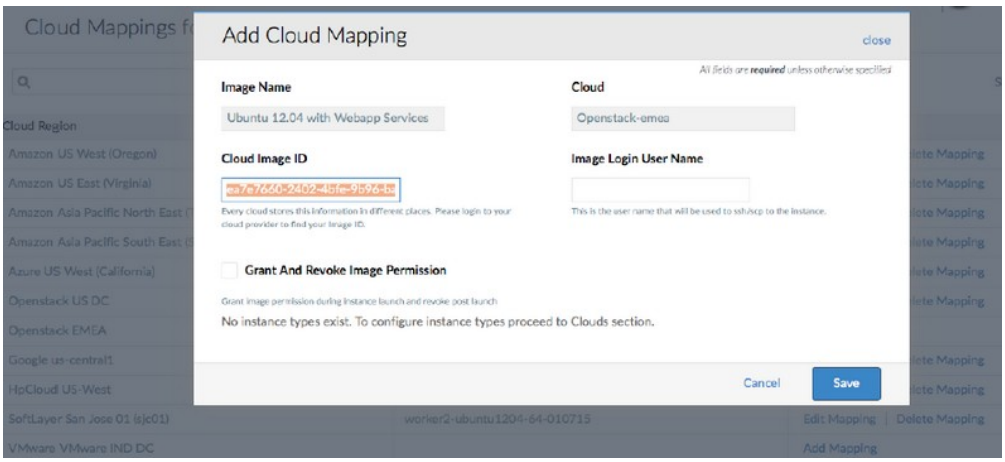
  完全な複製は送信元 VM または VM テンプレートで実行され、複製された VM はユーザが指定したデータストアまたはデータストア クラスタのいずれかに配置できます。

  詳細については、「VMware Configurations」を参照してください。

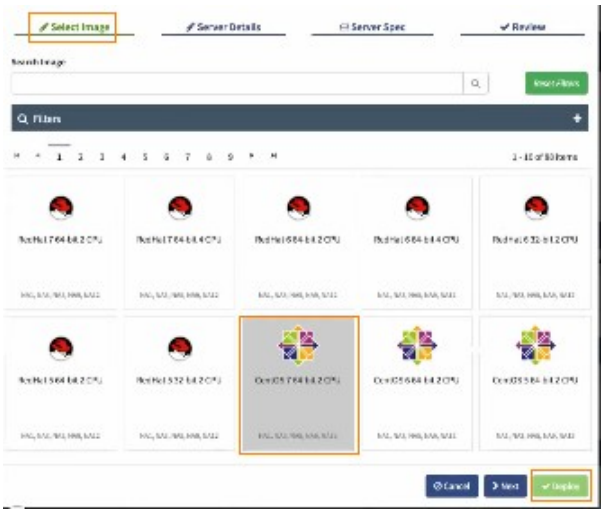
- OpenStack のイメージ ID

  - QCOW2 のイメージ ID(次の例で強調表示されたサンプル ID のマッピング):

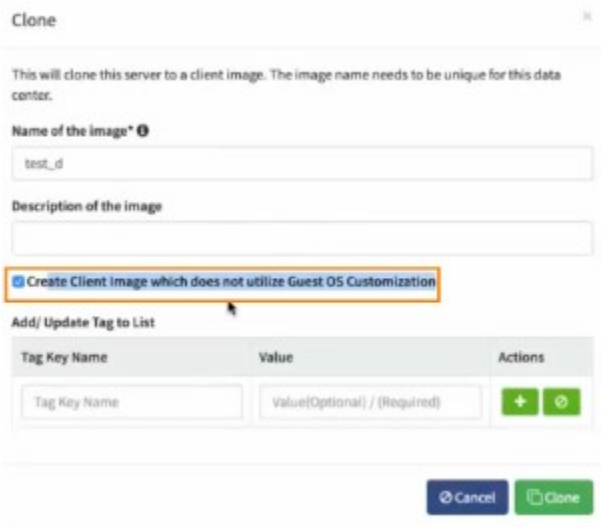




- 必要なイメージを使用して VM を作成、カスタマイズ、および展開します。



- VM インスタンスをシャットダウンし、インスタンスのクローンを作成します。



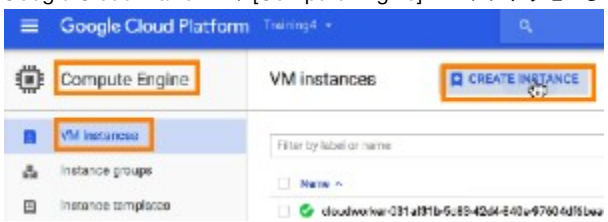
- Google のイメージ ID

  Google Cloud では、CloudCenter インスタンス用の VM を起動し、ページの一番下にある [REST] をクリックします。[REST] の出力に **sourceImage** の値を確認できます。

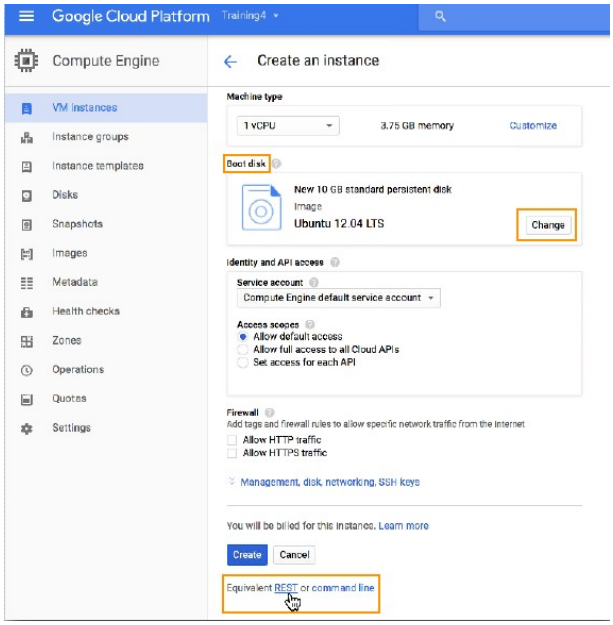
```
{
    "disks": [{
        "type": "PERSISTENT",
        "boot": true,
        "mode": "READ_WRITE",
        "autoDelete": true,
        "deviceName": "instance-1",
        "initializeParams": {
            "sourceImage":
"https://www.googleapis.com/compute/v1/projects/centos-cloud/global/images/cen
tos-7-v20160418",
            "diskType":
"projects/x-signifier-537/zones/us-central1-f/diskTypes/pd-ssd",
            "diskSizeGb": "10"
        }
    }]
}
```

  Google Cloud Platform の動的ブートストラップ機能を使用すると、REST ソースの詳細を使用してイメージの以前のバージョンに一時的にアクセスできるため、次の手順では、ソースを使用してイメージの詳細を取得し、CloudCenter イメージをマッピングすることができます。この方法を使用するには、次の手順を実行します。

  1. Google Cloud Platform の [Compute Engine] ページにアクセスして、[Create Instance] リンクをクリックします。



  2. [Create an instance] ページで、[Boot Disk] フィールドの [Change] をクリックします。

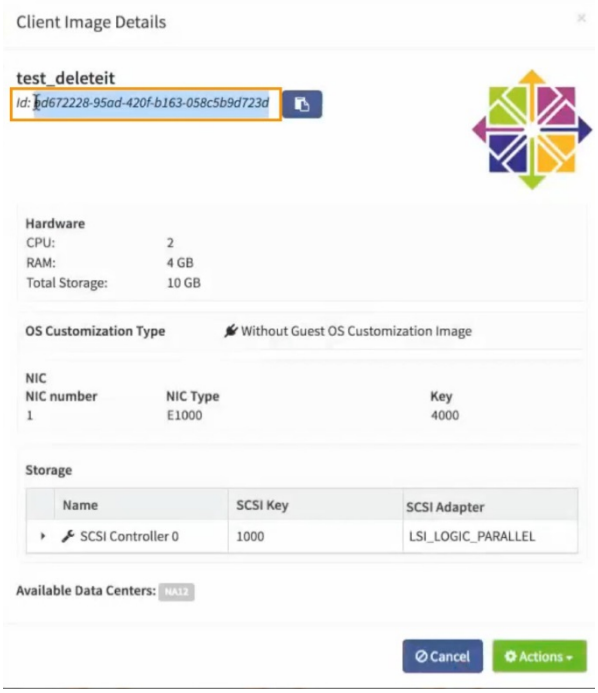


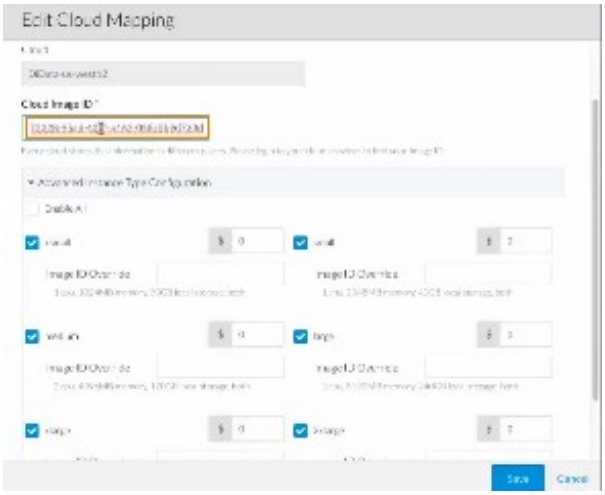
3. 環境の必要に応じて、次のオプション（動的ブートストラップはこれらのオプションに利用可能）のいずれかを選択し、変更を保存します。CentOS6 または 7、Ubuntu 12.04 または 14.04、Redhat Enterprise Linux 6 または 7、Windows 2008 または 2012
4. [Create an instance] ページに戻り、[REST] リンクをクリックします。同等の REST 要求が結果のポップアップに表示されます。
5. **sourceImage** の行まで下方向にスクロールし、この行に表示されるキーを選択します。

6. このキーをコピーして CCM UI の [イメージ マッピング（Image Mapping）] ページの [イメージ ID（Image ID）] フィールドに貼り付けます。

- Dimension Data のイメージ ID

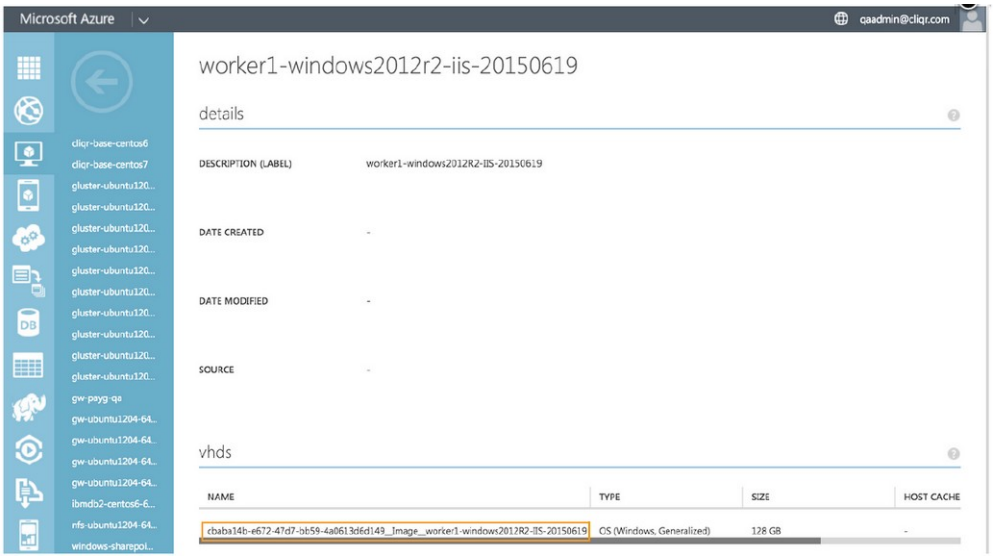
  Dimension Data で、**イメージ ID** は Dimension Data クラウド ポータルの [Client Image Details] ポップアップで表示される正確な名前です。必要な**イメージ**名をコピーして、Dimension Data クラウドの設定 プロセスの一部として CloudCenter CCM UI に貼り付けます。





- Azure Classic のイメージ ID

  Azure Classic では、アプリケーション VM イメージ マッピング名はディスク名です。ディスク名は、[Virtual instances] > [Image] タブをクリックし、リスト表示された名前を次のサンプル イメージで強調表示された [vhds] セクションにコピーして取得する必要があります。



- Azure RM のイメージ ID

  Azure RM で、次のコマンド出力（最新バージョン）は、CloudCenter プラットフォームに必要なイメージ ID を提供します。詳細については、htt ps://docs.microsoft.com/en-us/azure/virtual-machines/linux/cli-ps-findimage を参照してください。

  1. **標準の Azure RM イメージ**：次の例では、すべての CentOS 7.2 イメージに照会します。最新バージョンのイメージ ID は **OpenLogic:CentOS:7.2:7.2.20170105** です。

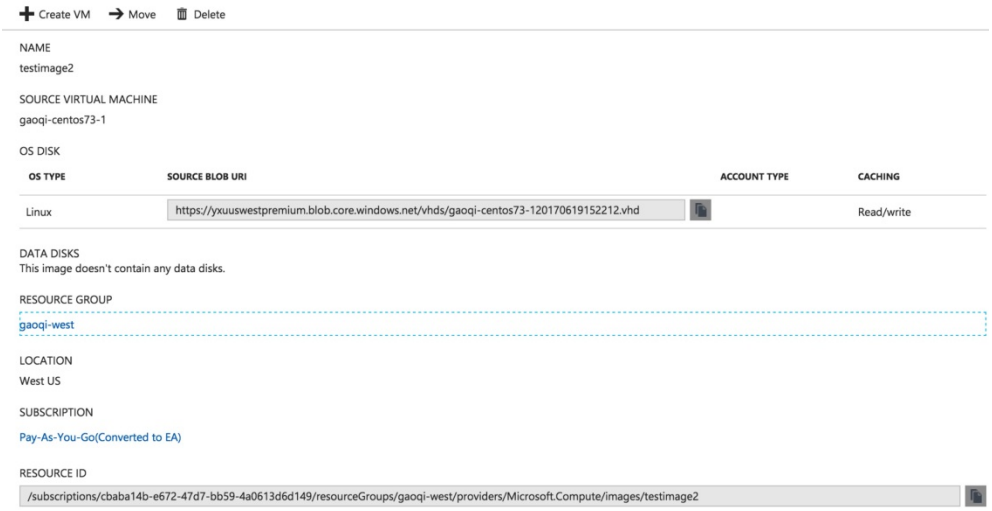
```
$ az vm image list -p OpenLogic --offer CentOS --sku 7.2 --all | more [
  {
    "offer": "CentOS",
    "publisher": "OpenLogic",
    "sku": "7.2",
    "urn": "OpenLogic:CentOS:7.2:7.2.20160303",
    "version": "7.2.20160303"
  },
  {
    "offer": "CentOS",
    "publisher": "OpenLogic",
    "sku": "7.2",
    "urn": "OpenLogic:CentOS:7.2:7.2.20160308",
    "version": "7.2.20160308"
  },
  {
    "offer": "CentOS",
    "publisher": "OpenLogic",
    "sku": "7.2",
    "urn": "OpenLogic:CentOS:7.2:7.2.20160620",
    "version": "7.2.20160620"
  },
  {
    "offer": "CentOS",
    "publisher": "OpenLogic",
    "sku": "7.2",
    "urn": "OpenLogic:CentOS:7.2:7.2.20161026",
    "version": "7.2.20161026"
  },
  {
    "offer": "CentOS",
    "publisher": "OpenLogic",
    "sku": "7.2",
    "urn": "OpenLogic:CentOS:7.2:7.2.20170105",
    "version": "7.2.20170105"
  },
  {
    "offer": "CentOS",
    "publisher": "OpenLogic",
    "sku": "7.2n",
    "urn": "OpenLogic:CentOS:7.2n:7.2.20160629",
    "version": "7.2.20160629"
  }
]
```

2. **カスタム Azure RM イメージ**:

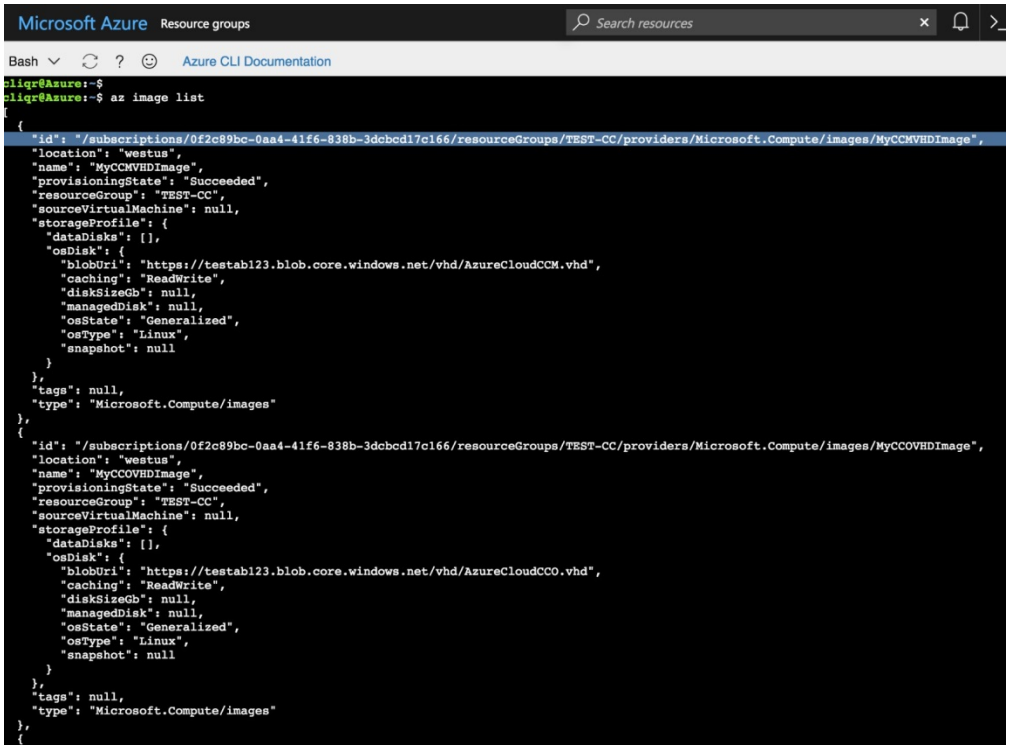
> **イメージ ID は CloudCenter バージョンによって異なります**
> イメージ ID は、CloudCenter バージョンによって異なります。
>
> a. CloudCenter 4.8.0 以前: イメージの **Blob Uri** をイメージ ID として使用します。
> b. CloudCenter 4.8.0.1 以降: イメージ ID としてイメージのリソース ID を使用します（新しい Azure SDK が含まれるため）。

> **管理型ストア オプション**
> カスタム Azure RM イメージを起動するには、記載されている管理対象ストレージ オプション（プレミアムまたは標準）のいずれかを選択する必要があります。
>
> 「Multiple Volumes」>「Azure RM Type Nuances」を参照してください

a. 次のスクリーンショットは、Azure RM UI を介したイメージ ID 取得画面を表示しています。



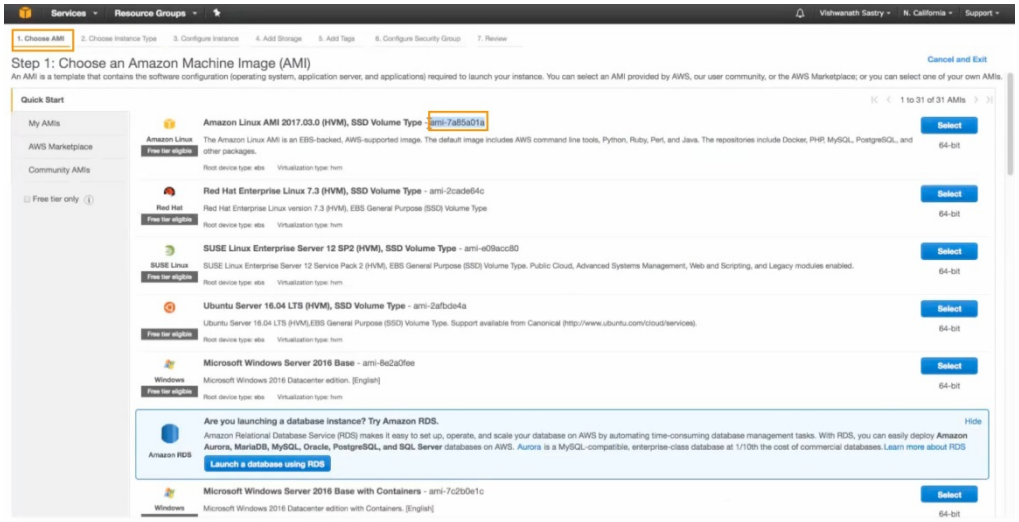
b. 次のスクリーンショットは、Azure RM CLI を介したイメージ ID 取得を表示しています。



> CloudCenter プラットフォームから既存の Azure Classic イメージを起動することはできません。まず、管理型ディスク機能を使用する前に、まず Azure RM に移行された Azure Classic イメージを移行する必要があります。

- AWS イメージ ID

  AWS では、イメージ ID は、AWS クラウド ポータルのマシン イメージ（AMI）ページに表示される正確な名前です。



ベース OS イメージをダウンロードおよびインポートして、イメージ ID を取得します

ワーカー アプライアンス用のイメージ ID を取得するには、次の手順に従います。

1. OVA または QCOW2 ファイルを software.cisco.com から /tmp フォルダにダウンロードします。詳細については、「仮想アプライアンスの概要」>「*インストール オプション*」を参照してください。
2. ワーカー アプライアンス用のイメージ ID を取得します。このイメージ ID は、CCM UI でイメージをマッピングするために必要です。

インストールに関する FAQ

- インストール プロセスにはどのくらいの時間がかかりますか。HA/非 HA/スタンドアロンではどうですか。
- 設定ウィザードで必須のパラメータはどれですか。
- パスワードを暗号化する必要はありますか。
- 外部モニタリング サービスを使用する方法を教えてください。
- CloudCenter アーキテクチャで自前のイメージを使用する方法を教えてください。
- 各イメージに管理エージェントをインストールする必要はありますか。
- CloudCenter プラットフォームのインストールの完了を確認する方法を教えてください。
- PostgreSQL インスタンスが CCM との通信を停止した場合、何ができますか。
- RHEL 7 のパッチを適用した後に PostgreSQL クラスタが起動しない場合、何ができますか。

インストール プロセスにはどのくらいの時間がかかりますか。HA/非 HA/スタンドアロンではどうですか。

次のエンドツーエンドのドキュメント プロセスに従う場合:

1. 仮想アプライアンスの概要を理解し、インストールする各コンポーネントに必要なモードとロールを選択する
2. 高可用性のベスト プラクティスを理解する
3. 「フェーズ 1:インフラストラクチャの準備」にリストされているインフラストラクチャを準備する
4. 「フェーズ 2:ファイアウォール ルールの設定」にリストされているネットワーク ルールを設定する
5. 「フェーズ 3:前提条件チェッカーの実行」にリストされているバリデータ チェックの*合格*を確認する
6. 「フェーズ 4:コンポーネントのインストール/設定」にリストされているようにインストールを実行する
7. 「CloudCenter の設定」にリストされているように CloudCenter プラットフォームを設定する

*「仮想アプライアンスの概要」で指定されたとおりに **VM の基本展開**をインストールするには、おおよそ次の時間がかかります。*

- HA インストール:約 3 日
- 非 HA インストール:約 1 日

設定ウィザードで必須のパラメータはどれですか。

必要なパラメータは、コンポーネント、ロール、およびモードによって異なります。各コンポーネントのウィザードは、必要に応じて、アスタリスク(*)で必須フィールドを識別しています。

パスワードを暗号化する必要はありますか。

ありません。CloudCenter は必要に応じてパスワードを暗号化するため、パスワードを暗号化するために何かをする必要はありません。

外部モニタリング サービスを使用する方法を教えてください。

クラウド ヘルス モニタ コンポーネントは、個々のコンポーネントの状態ではなくクラウドの状態を監視します。CloudCenter プラットフォームの状態を積極的にモニタし、継続的なパフォーマンスを確保するには、外部ツールを使用して、CCM と CCO の主要サービスを監視することができます。

- CCM の主要サービス:
  - Tomcat 8
  - PostgreSQL
  - MongoDB
- CCO の主要サービス:
  - Tomcat 8 – 各インスタンス上
  - MongoDB

詳細については、「Monitoring Best Practices」を参照してください。

CloudCenter アーキテクチャで自前のイメージを使用する方法を教えてください。

次の、該当する各ページを参照してください。

- Windows の場合:「Custom Windows Image」(インストーラ ファイルの手順を入手するには、CloudCenter サポート チームにお問い合わせください)。
- Linux の場合:「Custom Linux Image」(仮想アプライアンス ファイルは Linux イメージに使用できます)。

各イメージに管理エージェントをインストールする必要はありますか。

CloudCenter により管理される各 VM では、そこで動作する管理エージェント バンドル(エージェント)コンポーネントが必要です。CloudCenter プラットフォーム **インストーラ** ファイル内の各 VM イメージには管理エージェントが*含まれます*。CloudCenter プラットフォームは、エージェントがインストールされていないことを検出し、導入プロセスの一環として、各 VM にエージェントを自動的にプッシュします。

CloudCenter プラットフォームは管理エージェントで Java を使用します。Java のバージョンをアップグレードする必要があるかどうかを確認するには、「Management Agent Java Compatibility」の互換性マトリックスを参照してください。

CloudCenter プラットフォームのインストールの完了を確認する方法を教えてください。

このマイルストーンは、コンポーネントごとに異なります。

- **CCM**:CCM をインストールすると、CCM UI にアクセスして、管理者アカウントの設定を行うことができます。
- **CCO**:CCO コンポーネントをインストールすると、CCM に CCO を登録できます。
- **AMQP**:初めて AMQP コンポーネントをインストールする場合は、すべてのユーザが表示されることを確認するまで数分待つ必要があることがあります。`rabbitmqctl list_users` コマンド(「AMQP - Configure CCM/CCO Properties for Guacamole Server」に記載)によりすべてのユーザがリストされることを確認できます。

新しいアプリケーションを任意のクラウドにモデル化して導入したら、CloudCenter プラットフォームの インストール全体が成功と見なされます。

PostgreSQL インスタンスが CCM との通信を停止した場合、何ができますか。

HA モードの使用時にこのシナリオが発生した場合、この問題を解決するには次の手順に従います。

1. Postgres サービスを起動します。

```
systemctl start postgresql-9.5
```

2. .lock ファイルが必要なディレクトリに存在しないことを確認します。

```
cd /var/lib/pgsql/tmp/
# IF the PGSQL.lock is present, remove it using command
rm -rf *.lock
```

3. クラスタを停止して起動します。

```
pcs cluster stop
pcs cluster start
```

4. クラスタの状態を確認し、実行されていることを確認します。

```
pcs status
```

5. この問題が解決しない場合は、dbmaster と PGMasterVIP を再起動します。

```
pcs resource restart dbmaster
pcs resource restart PGMasterVIP
```

RHEL 7 のパッチを適用した後に PostgreSQL クラスタが起動しない場合、何ができますか。

RHEL 7 の MGMTPOSTGRES_MASTER と MGMTPOSTGRES_SLAVE の両方のサーバにパッチを適用している場合、両方のサーバを再起動した後にクラスタが起動しないという状況に遭遇することがあります。これはクラスタが同期されず、再起動後に自動的に起動できないことが原因です。

詳細については、「PostgreSQL Troubleshooting」を参照してください。