

# vCloud Director インストール、構成、およびアップグレード ガイド

2019 年 9 月 19 日

VMware Cloud Director 10.0

最新の技術ドキュメントは、VMware の Web サイト (<https://docs.vmware.com/jp/>)

**VMware, Inc.**  
3401 Hillview Ave.  
Palo Alto, CA 94304  
[www.vmware.com](http://www.vmware.com)

**ヴィエムウェア株式会社**  
105-0013 東京都港区浜松町 1-30-5  
浜松町スクエア 13F  
[www.vmware.com/jp](http://www.vmware.com/jp)

Copyright © 2010-2020 VMware, Inc. All rights reserved. [著作権および商標情報](#)。

# 目次

vCloud Director インストール、構成、およびアップグレード ガイド	7
<b>1 vCloud Director のインストール、構成、およびアップグレードの概要</b>	<b>8</b>
vCloud Director のアーキテクチャ	8
構成の計画	10
<b>2 vCloud Director のハードウェアおよびソフトウェア要件</b>	<b>11</b>
vCloud Director のネットワーク構成要件	12
ネットワーク セキュリティの要件	13
<b>3 vCloud Director のインストールまたは vCloud Director アプライアンスのデプロイ前</b>	<b>16</b>
Linux での vCloud Director の外部 PostgreSQL データベースの構成	16
転送サーバ ストレージの準備	18
RabbitMQ AMQP ブローカのインストールおよび構成	20
VMware パブリック キーのダウンロードとインストール	21
vCloud Director 用 NSX Data Center for vSphere のインストールと構成	21
vCloud Director 用 NSX-T Data Center のインストールと構成	22
<b>4 Linux 上の vCloud Director 向けの SSL 証明書の作成と管理</b>	<b>24</b>
Linux 上の vCloud Director に SSL 証明書を作成する前に	24
Linux 上での vCloud Director 用の自己署名付き SSL 証明書の作成	25
Linux 上での vCloud Director 用の CA 署名付き SSL 証明書キースタアの作成	26
Linux 上での vCloud Director 用にインポートされたプライベート キーを使用した、CA 署名付き SSL 証明書キースタアの作成	29
<b>5 Linux への vCloud Director のインストール</b>	<b>32</b>
サーバ グループの後続のメンバーへの vCloud Director のインストール	33
ネットワークおよびデータベース接続の構成	35
インタラクティブな設定に関するリファレンス	36
無人構成のリファレンス	37
応答ファイルの保護と再使用	40
サーバ グループの後続のメンバーへの vCloud Director のインストール	42
<b>6 vCloud Director アプライアンスのデプロイ</b>	<b>44</b>
アプライアンス環境とデータベースの高可用性構成	46
vCloud Director アプライアンスのデプロイの前提条件	48
vSphere Client を使用した vCloud Director アプライアンスのデプロイ	49

- [vCloud Director アプライアンスのサイジング ガイドライン 50](#)
- [vCloud Director アプライアンスのデプロイの開始 55](#)
- [vCloud Director アプライアンスのカスタマイズとデプロの終了 56](#)
- [VMware OVF Tool を使用した vCloud Director アプライアンスのデプロイ 59](#)

## 7 vCloud Director アプライアンス SSL 証明書の作成と管理 65

- [HTTPS 通信およびコンソール プロキシ通信用の署名付きワイルドカード証明書を使用した vCloud Director アプライアンスのデプロイ 65](#)
- [vCloud Director アプライアンスへの CA 署名付き SSL 証明書の作成とインポート 67](#)
- [プライベート キーおよび CA 署名付き SSL 証明書の vCloud Director アプライアンスへのインポート 70](#)
- [自己署名の組み込み PostgreSQL および vCloud Director アプライアンスの管理ユーザー インターフェイス証明書の置き換え 72](#)
- [vCloud Director アプライアンス証明書の更新 73](#)

## 8 vCloud Director アプライアンスの構成 75

- [データベースの高可用性クラスタ内のセルのステータスの表示 75](#)
- [高可用性クラスタのプライマリ データベース障害からのリカバリ 76](#)
- [高可用性クラスタのスタンバイ セル障害からのリカバリ 77](#)
- [vCloud Director アプライアンスの組み込みデータベースのバックアップとリストア 78](#)
  - [vCloud Director アプライアンス組み込みデータベースのバックアップ 78](#)
  - [高可用性データベース構成の vCloud Director アプライアンス環境のリストア 78](#)
- [vCloud Director データベースへの外部アクセスの設定 81](#)
- [vCloud Director アプライアンスへの SSH アクセスの有効化または無効化 82](#)
- [vCloud Director アプライアンスの DNS 設定の編集 82](#)
- [vCloud Director アプライアンス ネットワーク インターフェイスのスタティック ルートの編集 83](#)
- [vCloud Director アプライアンスの構成スクリプト 85](#)
- [vCloud Director アプライアンスの組み込み PostgreSQL データベースの容量の増加 85](#)
- [vCloud Director アプライアンスでの PostgreSQL 設定の変更 86](#)

## 9 高可用性クラスタ構成でのレプリケーション マネージャ ツール スイートの使用 88

- [データベース高可用性クラスタの接続ステータスの確認 88](#)
- [データベース高可用性クラスタのノードのレプリケーション ステータスの確認 90](#)
- [データベース高可用性クラスタのステータスの確認 90](#)
- [高可用性クラスタでオンラインに復帰した以前のプライマリ ノードの検出 92](#)
- [データベース高可用性クラスタ内のプライマリ セルおよびスタンバイ セルのロールの切り替え 94](#)
- [データベース高可用性クラスタ内の障害の発生したスタンバイ ノード、またはアクセスできないスタンバイ ノードの登録解除 95](#)
- [データベース高可用性クラスタ内の障害の発生したプライマリ セルの登録解除 95](#)
- [データベース高可用性クラスタ内の実行中のスタンバイ セルの登録解除 96](#)

## 10 セル管理ツール リファレンス 98

- [vCloud Director インストール環境の構成 101](#)

vCloud Director Web Console の有効化	103
レガシー API エンドポイントへのサービス プロバイダ アクセスの無効化	105
セルの管理	106
セル アプリケーションの管理	107
データベース接続プロパティを更新する	109
破損したスケジューラ データの検出および修復	111
HTTP およびコンソール プロキシ エンドポイントの自己署名証明書の生成	112
HTTP およびコンソール プロキシ エンドポイントの証明書の置き換え	114
外部サービスからの SSL 証明書のインポート	115
許可された SSL 暗号のリストの管理	116
許可された SSL プロトコルのリストの管理	118
メトリック収集の設定	119
Cassandra メトリック データベースの構成	122
システム管理者のパスワードの復元	123
タスクの失敗ステータスの更新	124
監査メッセージ処理の構成	125
電子メール テンプレートの構成	126
親なしの仮想マシンの検索	127
VMware カスタム エクスペリエンス改善プログラムへの参加または離脱	129
アプリケーションの設定の更新	130
カタログ同期のスロットリングの設定	131
vCloud Director ユーザー インターフェイスへのアクセスに失敗した場合のトラブルシューティング	132
vCenter Server 仮想マシン検出のデバッグ	133
マルチサイト拡張ネットワークの MAC アドレスの再生成	134
vCloud Director セルのデータベース IP アドレスの更新	136

## 11 vCloud Director のインストールまたは vCloud Director アプライアンスのデプロイ後 138

Microsoft Sysprep ファイルのサーバーへのインストール	138
vCloud Director アプライアンスのタイムゾーンの変更	139
公開アドレスのカスタマイズ	140
履歴メトリック データを格納するための Cassandra データベースのインストールと構成	142
外部 PostgreSQL データベースでの追加設定の実行	143

## 12 vCloud Director のアップグレード 145

vCloud Director アプライアンスのアップグレード	149
アップグレードが失敗した場合の vCloud Director アプライアンスのロールバック	151
VMware Update Repository を使用した vCloud Director アプライアンスのアップグレード	152
vCloud Director インストールの組織的なアップグレードの実行	154
vCloud Director インストールの手動アップグレード	156
vCloud Director セルのアップグレード	158
vCloud Director データベースのアップグレード	160

[データベース アップグレード ユーティリティ リファレンス](#) 161

### **13** vCloud Director アプライアンスへの移行 164

[外部 PostgreSQL データベースを使用する vCloud Director の vCloud Director アプライアンスへの移行](#)  
164

### **14** vCloud Director をアップグレードまたは移行した後に行う作業 169

[接続済み vCenter Server システムに関連付けられた各 NSX Manager のアップグレード](#) 169

[vCenter Server システム、ESXi ホスト、NSX Edge のアップグレード](#) 170

### **15** vCloud Director ログの表示 172

### **16** vCloud Director アプライアンスのトラブルシューティング 173

[vCloud Director アプライアンスのログ ファイルの調査](#) 173

[アプライアンスのデプロイ後に vCloud Director のセルの起動に失敗する](#) 174

[vCloud Director アプライアンスに移行またはリストアすると vCloud Director サービスの再構成に失敗する](#)  
174

[ログ ファイルを使用した vCloud Director のアップデートおよびパッチのトラブルシューティング](#) 175

[vCloud Director のアップデートの確認に失敗する](#) 175

[vCloud Director の最新アップデートのインストールに失敗する](#) 176

### **17** vCloud Director ソフトウェアのアンインストール 177

# vCloud Director インストール、構成、およびアップグレード ガイド

vCloud Director インストール、構成、およびアップグレード ガイド は、VMware vCloud Director<sup>®</sup> for Service Providers ソフトウェアのインストールとアップグレード、および VMware vSphere<sup>®</sup>、VMware NSX<sup>®</sup> for vSphere<sup>®</sup>、および VMware NSX-T<sup>™</sup> Data Center と連携させるための構成についての情報を提供します。

## 対象読者

『vCloud Director インストール、構成、およびアップグレード ガイド』は、vCloud Director ソフトウェアをインストールまたはアップグレードする必要があるすべてのユーザーを対象にしています。本書の情報は、Linux、Windows、IP ネットワーク、および vSphere に精通した、経験豊富なシステム管理者向けに書かれています。

# vCloud Director のインストール、構成、およびアップグレードの概要

# 1

1 つ以上の Linux サーバに vCloud Director ソフトウェアをインストールするか、vCloud Director アプライアンスの 1 つ以上のインスタンスをデプロイして、vCloud Director サーバ グループを作成します。インストール プロセス中に、最初の vCloud Director 構成を実行します。これには、ネットワーク接続とデータベース接続の確立が含まれます。

Linux 用の vCloud Director ソフトウェアには外部データベースが必要ですが、vCloud Director アプライアンスでは組み込みの PostgreSQL データベースが使用されます。

vCloud Director サーバ グループを作成したら、vSphere リソースに vCloud Director インストールを統合します。ネットワーク リソースの場合、vCloud Director は NSX Data Center for vSphere、NSX-T Data Center、またはその両方を使用できます。

既存の vCloud Director インストールをアップグレードすると、vCloud Director ソフトウェアとデータベーススキーマが更新され、サーバ、データベース、および vSphere 間の既存の関係は元のまま維持されます。

Linux 上の既存の vCloud Director インストールを vCloud Director アプライアンスに移行する場合は、vCloud Director ソフトウェアを更新し、データベースをアプライアンス内の組み込みデータベースに移行します。

この章には、次のトピックが含まれています。

- [vCloud Director のアーキテクチャ](#)
- [構成の計画](#)

## vCloud Director のアーキテクチャ

vCloud Director サーバ グループは、Linux または vCloud Director アプライアンスのデプロイにインストールされている 1 台以上の vCloud Director サーバで構成されます。グループの各サーバーは vCloud Director セルと呼ばれる一連のサービスを実行します。すべてのセルは、1 つの vCloud Director データベースおよび転送サーバ ストレージを共有し、vSphere およびネットワーク リソースに接続します。

---

**重要：** Linux 上の vCloud Director インストールおよび vCloud Director アプライアンス環境を 1 つのサーバグループ内で混在させることはできません。

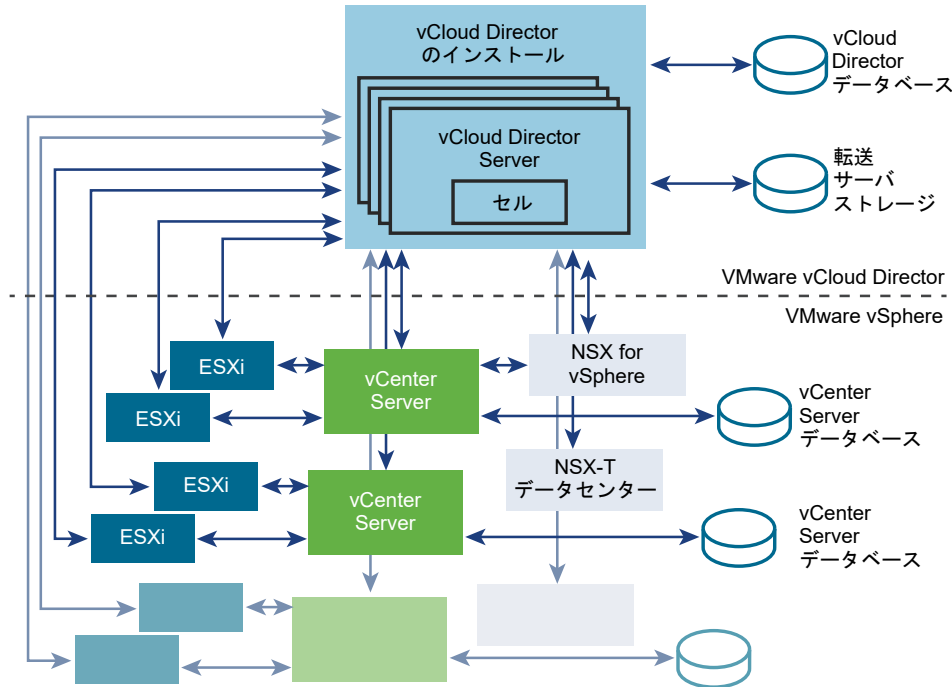
---

vCloud Director の高可用性を確保するには、1 つのサーバ グループに複数の vCloud Director セルをインストールする必要があります。サードパーティのロード バランサを使用する場合は、ダウンタイムなしの自動フェイルオーバーを確保できます。



vCloud Director インストールは、複数の VMware vCenter Server<sup>®</sup> システム、およびそれらのシステムによって管理される VMware ESXi<sup>™</sup> ホストに接続できます。ネットワーク サービスに関しては、vCloud Director は vCenter Server に関連付けられた NSX Data Center for vSphere を使用できます。または、vCloud Director に NSX-T Data Center を登録できます。NSX Data Center for vSphere と NSX-T Data Center の混在もサポートされます。

図 1-1. vCloud Director アーキテクチャ図



Linux にインストールされた vCloud Director サーバ グループは、外部データベースを使用します。

アプライアンス環境で構成される vCloud Director サーバ グループでは、サーバ グループの最初のメンバーの組み込みデータベースが使用されます。アプライアンスの 2 つのインスタンスを同じサーバ グループ内のスタンバイセルとしてデプロイすることにより、vCloud Director データベースに高可用性を構成することができます。[アプライアンス環境とデータベースの高可用性構成](#)を参照してください。

図 1-2. 組み込みデータベースの高可用性クラスターで構成された vCloud Director アプライアンス

vCloud Director のインストールと設定のプロセスでは、セルが作成され、それらのセルが共有データベースおよび転送サーバ ストレージに接続され、システム管理者アカウントが作成されます。その後、システム管理者が vCenter Server システム、ESXi ホスト、および NSX Manager または NSX-T Manager インスタンスへの接続を確立します。

vSphere およびネットワーク リソースの追加の詳細については、『vCloud Director Service Provider Admin Portal Guide』を参照してください。

## 構成の計画

vSphere は、vCloud Director にストレージ、コンピューティング、およびネットワーク キャパシティを提供します。インストールを開始する前に、クラウドで vSphere および vCloud Director のキャパシティがどの程度必要になるかを検討し、それをサポートできる構成を計画します。

構成要件は、クラウド内の組織数、各組織内のユーザー数、それらのユーザーのアクティビティ レベルなど、多くの要素に応じて変わります。一般的な構成の場合、基本として次のガイドラインを参考にしてください。

- クラウド内でアクセス可能にする vCenter Server システムごとに 1 つの vCloud Director セルを割り当てます。
- すべてのターゲット vCloud Director Linux サーバが、メモリおよびストレージの最小要件を満たしていることを確認します（vCloud Director リリース ノートを参照）。
- Linux に vCloud Director をインストールする場合は、[Linux での vCloud Director の外部 PostgreSQL データベースの構成](#)の説明に沿って vCloud Director データベースを設定します。

# vCloud Director のハードウェアおよびソフトウェア要件

## 2

vCloud Director サーバ グループの各サーバは、特定のハードウェアおよびソフトウェア要件を満たす必要があります。さらに、グループの全メンバーがサポート対象のデータベースにアクセスできる必要があります。各サーバ グループには、vCenter Server システム、NSX Manager インスタンス、および 1 つまたは複数の ESXi ホストへのアクセスが必要です。

## 他の VMware 製品との互換性

vCloud Director と他の VMware 製品との互換性に関する最新情報については、[http://partnerweb.vmware.com/comp\\_guide/sim/interop\\_matrix.php](http://partnerweb.vmware.com/comp_guide/sim/interop_matrix.php) の『VMware 製品の相互運用性マトリックス』を参照してください。

## vSphere 構成要件

vCloud Director で使用する vCenter Server インスタンスおよび ESXi ホストは、特定の構成要件を満たす必要があります。

- vCloud Director の外部ネットワークまたはネットワーク プールとして使用する vCenter Server ネットワークは、vCloud Director で使用するクラスタ内のすべてのホストから使用できる必要があります。これらのネットワークをデータセンター内のすべてのホストから使用できるようにすることで、新しい vCenter Server インスタンスを vCloud Director に追加するタスクが簡素化されます。
- 隔離されたネットワークおよび NSX Data Center for vSphere にバックアップされるネットワーク プールには、vSphere Distributed Switch が必要です。
- vCloud Director で使用する vCenter Server クラスタには、vSphere DRS 自動化レベルとして [完全自動化] を指定する必要があります。Storage DRS が有効になっている場合は、どの自動化レベルでも Storage DRS を構成できます。
- vCenter Server インスタンスは、そのホストを信頼する必要があります。vCloud Director によって管理されるすべてのクラスタのすべてのホストは、検証されたホスト証明書が必要とされるように構成する必要があります。特に、すべてのホストで一致するサンプリントを決定、比較、および選択する必要があります。『vCenter Server とホスト管理』ドキュメントの「SSL 設定の構成」を参照してください。

## vSphere ライセンス要件

vCloud Director Service Provider Bundle に、必要な vSphere ライセンスが含まれています。

## サポートされているプラットフォーム、データベース、ブラウザ

このリリースの vCloud Director でサポートされているサーバ プラットフォーム、ブラウザ、LDAP サーバ、およびデータベースに関する詳細については、『vCloud Director 10.0 リリース ノート』を参照してください。

## ディスク容量、メモリ、および CPU の要件

ディスク容量、メモリ、CPU などの vCloud Director セルの物理要件は、『vCloud Director 10.0 リリース ノート』に示されています。

## 共有ストレージ

NFS またはその他の vCloud Director 転送サービス向け共有ストレージ ボリューム。ストレージ ボリュームは拡張可能で、サーバ グループ内のすべてのサーバにアクセスできる必要があります。

この章には、次のトピックが含まれています。

- [vCloud Director のネットワーク構成要件](#)
- [ネットワーク セキュリティの要件](#)

## vCloud Director のネットワーク構成要件

vCloud Director の安全で信頼性の高い操作には、ホスト名の正引き参照/逆引き参照やネットワーク タイム サービスなどのサービスをサポートする安全で信頼性の高いネットワークが不可欠です。vCloud Director のインストールを開始する前に、ネットワークがこれらの要件を満たしている必要があります。

vCloud Director サーバ、データベース サーバ、vCenter Server システム、NSX コンポーネントを接続するネットワークは、以下に示すいくつかの要件を満たす必要があります。

### IP アドレス

各 vCloud Director サーバは、2 つの異なる SSL エンドポイントとして動作可能である必要があります。1 つは、HTTP サービス用エンド ポイント、もう 1 つは、コンソール プロキシ サービス用エンド ポイントです。これらのエンド ポイントには異なる IP アドレスを割り当てることもできますし、同じ IP アドレスで 2 つの異なるポートを割り当てることもできます。これらのアドレスの作成に、IP エイリアスや複数のネットワーク インターフェイスを使用できます。2 つ目のアドレス作成には、Linux の `ip addr add` コマンドを使用しないでください。

vCloud Director アプライアンスは、コンソール プロキシ サービスに `eth0` IP アドレスとカスタム ポート 8443 を使用します。

### コンソール プロキシ アドレス

コンソール プロキシ エンドポイントとして構成される IP アドレスは、SSL 終了ロード バランサまたはリバース プロキシの背後に置かないでください。すべてのコンソール プロキシ要求は、コンソール プロキシ IP アドレスに直接、リレイする必要があります。

単一の IP アドレスを使用するインストールでは、Service Provider Admin Portal でコンソール プロキシ アドレスをカスタマイズできます。たとえば、vCloud Director アプライアンスのコンソール プロキシ アドレスを `vcloud.example.com:8443` にカスタマイズする必要があります。

## ネットワーク タイム サービス

NTP のようなネットワーク タイム サービスを使用して、データベース サーバーを含むすべての vCloud Director サーバーのクロックを同期させる必要があります。同期されるサーバーのクロック間で許容されるずれは最大 2 秒です。

## サーバーのタイム ゾーン

データベース サーバーを含むすべての vCloud Director サーバーを同じタイム ゾーンで構成する必要があります。

## ホスト名の解決

インストールおよび構成時に指定したすべてのホスト名は、DNS で完全修飾ドメイン名または非修飾ホスト名の正引き/逆引きを使用して解決できる必要があります。たとえば、`vcloud.example.com` という名前のホストの場合、vCloud Director ホスト上で次のコマンドが両方とも正常に実行される必要があります。

```
nslookup vcloud
nslookup vcloud.example.com
```

さらに、ホスト `mycloud.example.com` の IP アドレスが 192.168.1.1 の場合、次のコマンドから `vcloud.example.com` が返される必要があります。

```
nslookup 192.168.1.1
```

アプライアンスには、eth0 IP アドレスの DNS 逆引き機能が必要です。使用環境内で次のコマンドが成功する必要があります。

```
host -W 15 -R 1 -T <eth0-IP-address>
```

## ネットワーク セキュリティの要件

vCloud Director を安全に操作するには、安全なネットワーク環境が必要です。このネットワーク環境を、vCloud Director のインストールを開始する前に構成してテストします。

すべての vCloud Director サーバーを、セキュリティで保護し監視されているネットワークに接続します。  
vCloud Director ネットワーク接続には、いくつかの追加要件があります。

- vCloud Director を公開インターネットに直接接続しないでください。vCloud Director ネットワーク接続を、常時ファイアウォールで保護します。受信接続に対して開くのはポート 443 (HTTPS) のみにする必要があります。必要に応じてポート 22 (SSH) と 80 (HTTP) も受信接続に対して開くことができます。また、`cell-management-tool` ではセルのループバック アドレスにアクセスする必要があります。JMX への要求（ポート 8999）を含む、公開ネットワークから受信した他のすべてのトラフィックは、ファイアウォールで拒否する必要があります。

表 2-1. vCloud Director ホストからの受信パケットを許容する必要があるポート

ポート	プロトコル	コメント
111	TCP、UDP	転送サービスで使用する NFS ポートマッパー
920	TCP、UDP	転送サービスで使用する NFS rpc.statd
61611	TCP	AMQP
61616	TCP	AMQP

- 送信接続に使用されるポートを公開ネットワークに接続しないでください。

表 2-2. vCloud Director ホストからの送信パケットを許容する必要があるポート

ポート	プロトコル	コメント
25	TCP、UDP	SMTP
53	TCP、UDP	DNS
111	TCP、UDP	転送サービスで使用する NFS ポートマッパー
123	TCP、UDP	NTP
389	TCP、UDP	LDAP
443	TCP	標準ポートを使用した vCenter Server、NSX Manager、および ESXi の各接続。これらのサービス用に異なるポートを選択した場合は、ポート 443 への接続を無効にし、選択したポートでこれらのサービスでできるように設定します。
514	UDP	任意。syslog の使用を有効にします。
902	TCP	vCenter および ESXi 接続。
903	TCP	vCenter および ESXi 接続。
920	TCP、UDP	転送サービスで使用する NFS rpc.statd。
5432	TCP	デフォルトの PostgreSQL データベース ポート
5672	TCP、UDP	任意。タスク拡張用 AMQP メッセージ。

表 2-2. vCloud Director ホストからの送信パケットを許容する必要があるポート (続き)

ポート	プロトコル	コメント
61611	TCP	AMQP
61616	TCP	AMQP

- 専用のプライベート ネットワーク上で、vCloud Director サーバと次のサーバ間のトラフィックを経路指定します。
  - vCloud Director データベース サーバ
  - RabbitMQ
  - Cassandra
- 可能な場合は、専用のプライベート ネットワーク上で、vCloud Director サーバ、vSphere、および NSX 間のトラフィックを経路指定します。
- プロバイダ ネットワークをサポートする仮想スイッチと分散仮想スイッチは、互いに分離する必要があります。この間で同じレイヤー 2 の物理ネットワーク セグメントを共有することはできません。
- 転送サービス ストレージに NFSv4 を使用します。最も一般的な NFS のバージョンである NFSv3 は、転送時の暗号化が提供されないため、一部の構成ではデータの転送中に傍受または改ざんを受ける可能性があります。NFSv3 に固有の脅威については、SANS のホワイト ペーパー [NFS Security in Both Trusted and Untrusted Environments](#) に記載されています。vCloud Director の転送サービスの設定とセキュリティ強化についての詳細は、VMware ナレッジベースの記事 [KB2086127](#) に記載されています。

# vCloud Director のインストールまたは vCloud Director アプライアンスのデプロイ前

## 3

Linux サーバに vCloud Director をインストールするか、vCloud Director アプライアンスをデプロイする前に、環境を準備する必要があります。

この章には、次のトピックが含まれています。

- [Linux での vCloud Director の外部 PostgreSQL データベースの構成](#)
- [転送サーバストレージの準備](#)
- [RabbitMQ AMQP ブローカのインストールおよび構成](#)
- [VMware パブリック キーのダウンロードとインストール](#)
- [vCloud Director 用 NSX Data Center for vSphere のインストールと構成](#)
- [vCloud Director 用 NSX-T Data Center のインストールと構成](#)

## Linux での vCloud Director の外部 PostgreSQL データベースの構成

vCloud Director セルでは、共有情報の保存にデータベースを使用します。Linux で vCloud Director をインストールする前に、PostgreSQL データベース インスタンスをインストールおよび設定して、vCloud Director データベース ユーザー アカウントを作成する必要があります。

PostgreSQL データベースを vCloud Director と一緒に使用する場合、特定の構成要件があります。

vCloud Director を使用するには、個別の専用データベース スキーマを作成する必要があります。vCloud Director では、他の VMware 製品とデータベース スキーマを共有することはできません。

vCloud Director は、PostgreSQL データベースへの SSL 接続をサポートします。ネットワークおよびデータベース接続の無人での構成中に、または vCloud Director サーバ グループの作成後に、PostgreSQL データベースで SSL を有効にできます。 [無人構成のリファレンス](#)および [外部 PostgreSQL データベースでの追加設定の実行](#)を参照してください。

---

**注：** 外部データベースを使用するのは、Linux 上の vCloud Director のみです。vCloud Director アプライアンスは、組み込みの PostgreSQL データベースを使用します。

---



## 前提条件

サポートされている vCloud Director データベースについては、[VMware 製品の相互運用性マトリックス](#) を参照してください。

PostgreSQL コマンド、スクリプト、および操作に習熟していることを前提としています。

## 手順

### 1 データベース サーバーを構成します。

16 GB のメモリ、100 GB のストレージ、4 つの CPU を搭載したデータベース サーバは、一般的な vCloud Director サーバ グループに適しています。

### 2 サポートされている PostgreSQL のディストリビューションをデータベース サーバにインストールします。

- データベースの SERVER\_ENCODING 値は、UTF-8 にする必要があります。この値はデータベースのインストール時に設定され、データベース サーバのオペレーティング システムで使用されているエンコードと常に一致します。
- PostgreSQL initdb コマンドを使用すると、LC\_COLLATE と LC\_CTYPE の値を en\_US.UTF-8 に設定できます。以下にその例を挙げます。

```
initdb --locale=en_US.UTF-8
```

### 3 データベース ユーザーを作成します。

次のコマンドを実行すると、ユーザー vcloud が作成されます。

```
create user vcloud;
```

### 4 データベース インスタンスを作成し、所有者を設定します。

次のようなコマンドを使用して、vcloud という名前のデータベース ユーザーをデータベース所有者として指定します。

```
create database vcloud owner vcloud;
```

### 5 データベース パスワードをデータベース所有者アカウントに割り当てます。

次のコマンドにより、パスワード vcloudpass がデータベース所有者 vcloud に割り当てられます。

```
alter user vcloud password 'vcloudpass';
```

### 6 データベース所有者がデータベースにログインできるようにします。

次のコマンドにより、login オプションがデータベース所有者 vcloud に割り当てられます。

```
alter role vcloud with login;
```

## 次のステップ

vCloud Director サーバ グループを作成した後、PostgreSQL データベースを構成して vCloud Director セルからの SSL 接続を要求し、一部のデータベース パラメータを調整して最適なパフォーマンスを確保することができます。外部 [PostgreSQL データベースでの追加設定の実行](#) を参照してください。

## 転送サーバ ストレージの準備

アップロード、ダウンロードおよび外部に公開またはサブスクライブされているカタログ項目の一時的なストレージを提供するために、NFS またはその他の共有ストレージ ポリ्यूームは vCloud Director サーバ グループ内のすべてのサーバからアクセスする必要があります。

---

**重要：** vCloud Director アプライアンスは、NFS タイプの共有ストレージのみをサポートします。アプライアンスのデプロイ プロセスには、NFS 共有転送サーバ ストレージのマウントが含まれます。

---

NFS を転送サーバ ストレージに使用する場合、NFS ベースの転送サーバ ストレージをマウントして使用するには、vCloud Director サーバ グループの各 vCloud Director セルを構成する必要があります。NFS ベースの場所をマウントし、転送サーバ ストレージとして使用するよう各セルを設定するには、個々のユーザーおよびグループの権限が必要です。

サーバ グループの各メンバーは、このポリ्यूームを同じマウントポイント（通常は `/opt/vmware/vcloud-director/data/transfer`）にマウントします。このポリ्यूームの領域は、次の 2 通りの方法で消費されます。

- 転送中に、アップロードとダウンロードがこのストレージを占有します。転送が完了すると、アップロードとダウンロードはストレージから削除されます。60 分間進行のない転送は、期限切れとしてマーキングされ、システムによってクリーンアップされます。大きいイメージが転送される可能性があるため、この用途には少なくとも数百ギガバイトを割り当てることをお勧めします。
- 外部に公開され、公開されたコンテンツのキャッシュが有効にされているカタログ内のカタログ アイテムが、このストレージを占有します。外部に公開されても、キャッシュを有効にしていないカタログ アイテムは、このストレージを占有しません。クラウド内の組織に対し、外部公開されるカタログの作成を許可すると、数百あるいは数千のカタログ アイテムがこのポリ्यूーム上の容量を必要とすると想定できます。各カタログ アイテムのサイズは、圧縮された OVF 形式の仮想マシン程度のサイズです。

---

**注：** 転送サーバ ストレージのポリ्यूームには、将来の拡張のための容量が必要です。

---

## vCloud Director が転送サーバ ストレージの場所に対してファイル システム権限を使用する方法

vCloud Director サーバ グループ内のすべての vCloud Director セル：

- カatalogへのアイテムのアップロードなどの標準的なクラウド操作では、vCloud Director セルのデーモンが vcloud グループの vcloud ユーザーを使用して、転送サーバ ストレージとの間でファイルの読み取りおよび書き込みを行います。vcloud ユーザーは、`umask 0077` でファイルを書き込みます。vCloud Director インストーラが実行されてサーバ グループ メンバーに vCloud Director ソフトウェアがインストールされるとき、vcloud ユーザーと vcloud グループも作成されます。

- vCloud Director ログ データ コレクタ スクリプト `vmware-vcd-support` は、1 回の操作ですべての vCloud Director セルからログを収集して 1 つの `tar.gz` ファイルにまとめることができます。このスクリプトを実行すると、生成された `tar.gz` ファイルは、スクリプトを呼び出したユーザーのユーザー ID を使用して転送サーバ ストレージ上のディレクトリに書き込まれます。デフォルトでは、スクリプトを実行する権限を持つユーザーは root ユーザーだけです。
- このセルの root ユーザーが実行するスクリプトは、転送サーバ ストレージ上の `vmware-vcd-support` ディレクトリに `tar.gz` ファイルを書き込みます。複数セルのオプションを使用してすべてのセルから一度にログを収集する場合、root ユーザーには、`tar.gz` の診断ログ バンドルを取得するための読み取り権限が必要です。

## NFS サーバを構成するための要件

NFS サーバの構成には、vCloud Director が NFS ベースの転送サーバ ストレージの場所との間でファイルの読み書きができるようにするための特定の要件があります。これにより、vcloud ユーザーは標準的なクラウド操作を実行でき、root ユーザーは複数セルのログ収集を実行できます。

- NFS サーバのエクスポート リストでは、vCloud Director サーバ グループ内の各サーバ メンバーが、エクスポート リストで指定された共有の場所に対する読み取り/書き込みアクセス権を持つようにする必要があります。このアクセス権により、vcloud ユーザーは共有の場所との間でファイルの読み取りおよび書き込みを実行できます。
- NFS サーバでは、vCloud Director サーバ グループ内の各サーバ上の root システム アカウントによる共有場所への読み取り/書き込みアクセスを許可する必要があります。このアクセス権により、`vmware-vcd-support` スクリプトでマルチ セル オプションを使用することで 1 つのバンドル内のすべてのセルからのログを一度に収集できます。この要件は、この共有の場所の NFS エクスポート構成で `no_root_squash` を使用することで満たすことができます。

たとえば、NFS サーバの IP アドレスが `192.168.120.7` で、vCloud Director サーバ グループ用の転送領域として `/nfs/vCDspace` の場所に `vCDspace` という名前のディレクトリがある場合、このディレクトリをエクスポートするには、その所有権と権限が `root:root` および `750` であることを確認する必要があります。`vcd-cell1-IP` と `vcd-cell2-IP` という名前の 2 つのセルに共有場所への読み取り/書き込みアクセスを許可する方法は、`no_root_squash` メソッドです。`/etc/exports` ファイルに行を追加する必要があります。

```
192.168.120.7/nfs/vCDspace vCD_Cell1_IP_Address(rw,sync,no_subtree_check,no_root_squash)
vCD_Cell2_IP_Address(rw,sync,no_subtree_check)
```

このエクスポート行で、セルの IP アドレスとその直後の左括弧との間には空白文字を置きません。セルから共有の場所にデータが書き込まれているときに NFS サーバを再起動した場合、エクスポート設定で `sync` オプションを使用していると共有場所のデータの破損を避けることができます。エクスポート設定で `no_subtree_check` オプションを使用すると、ファイル システムのサブディレクトリがエクスポートされときの信頼性が向上します。

vCloud Director サーバ グループの各サーバは、NFS エクスポートのエクスポート リストを調べることによって NFS シェアのマウントが許可される必要があります。`exportfs -a` を実行することによってマウントをエクスポートして、すべての NFS 共有を再エクスポートします。NFS デーモン `rpcinfo -p localhost` または `service nfs status` がサーバ上で実行されている必要があります。

## vCloud Director インストールを新しいバージョンにアップグレードする際の考慮事項

vCloud Director サーバ グループのアップグレードでは、アップグレードするバージョンのインストール ファイルを実行すると vCloud Director サーバ グループのすべてのメンバーがアップグレードされます。転送サーバ ストレージの場所にはすべてのセルがアクセスできるため、組織によっては処理の都合上、アップグレード用のインストール ファイルをこの場所にダウンロードし、そこから実行します。アップグレード インストール ファイルを実行するには root ユーザーを使用する必要があるため、アップグレードを実行するために転送サーバ ストレージの場所を使用する場合は、アップグレード実行時に root ユーザーがアップグレード インストール ファイルを実行できることを確認する必要があります。root ユーザーとしてアップグレードを実行できない場合は、NFS マウントの外のディレクトリなど、root ユーザーとして実行できる別の場所にファイルをコピーする必要があります。

## RabbitMQ AMQP ブローカのインストールおよび構成

AMQP (Advanced Message Queuing Protocol) は、エンタープライズ システムでの柔軟なメッセージングをサポートするメッセージ キューイングのオープン標準です。vCloud Director は RabbitMQ AMQP ブローカを使用して、拡張サービス、オブジェクト拡張、および通知に使用されるメッセージ バスを提供します。

### 手順

- 1 <https://www.rabbitmq.com/download.html> から RabbitMQ Server をダウンロードします。

サポートされている RabbitMQ リリースのリストについては、『vCloud Director リリース ノート』を参照してください。

- 2 RabbitMQ インストールの手順に基づいて、RabbitMQ をサポートされるホストにインストールします。

RabbitMQ サーバー ホストは、それぞれの vCloud Director セルによりネットワーク上で到達可能でなければなりません。

- 3 RabbitMQ インストール中に、この RabbitMQ インストールと連携するように vCloud Director を構成するときに必要となる値を書き留めておきます。

- RabbitMQ サーバ ホストの完全修飾ドメイン名。例: *amqp.example.com*。
- RabbitMQ を認証するために有効なユーザー名とパスワード。
- ブローカーがメッセージをリスンするポート。デフォルトは、5672 です。
- RabbitMQ 仮想ホスト。デフォルトは、`/` です。

### 次のステップ

デフォルトでは、vCloud Director AMQP サービスは暗号化されていないメッセージを送信します。SSL を使用してこれらのメッセージを暗号化するように AMQP サービスを構成できます。vCloud Director セルで Java ランタイム環境のデフォルトの JCEKS トラスト ストアを使用して、ブローカ証明書（通常は `$VCLLOUD_HOME/jre/lib/security/cacerts`）を検証するようにサービスを構成することもできます。

vCloud Director AMQP サービスで SSL を有効にするには、以下の手順を実行します。

- 1 vCloud Director Service Provider Admin Portal のメイン メニュー (≡) から、[管理] を選択します。

- 2 左側のパネルの [設定] で、[拡張性] をクリックします。
- 3 [拡張性] をクリックし、[AMQP ブローカー] セクションの [編集] をクリックします。
- 4 [SSL を使用] トグルを有効にします。
- 5 [すべての証明書を受け入れる] トグルを有効にするか、次のいずれかを指定します。
  - SSL 証明書のパス名
  - JCEKS トラスト ストアのパス名とパスワード

## VMware パブリック キーのダウンロードとインストール

インストール ファイルはデジタル署名されています。この署名を検証するためには、VMware パブリック キーをダウンロードし、インストールする必要があります。

Linux rpm ツールと VMware パブリック キーを使用して、vCloud Director インストール ファイルのデジタル署名を検証し、vmware.com からダウンロードされた署名付きの他のファイルを検証することができます。vCloud Director をインストールする予定のコンピュータにパブリック キーをインストールする場合、検証はインストールまたはアップグレードの一部として行われます。インストールやアップグレード手順を開始する前に署名を手動で検証し、すべてのインストールまたはアップグレードに検証済みのファイルを使用することもできます。

**注：** ダウンロード サイトはまた、ダウンロードのチェックサム値も発行します。チェックサムは 2 つの共通方法で発行されます。チェックサムの検証は、ダウンロードしたファイルのコンテンツが投稿されたコンテンツと同じであることを検証します。デジタル署名を検証しません。

### 手順

- 1 VMware パッケージ パブリック キーを保存するためにディレクトリを作成します。
- 2 Web ブラウザを使用して <http://packages.vmware.com/tools/keys> ディレクトリからすべての VMware パブリック パッケージ パブリック キーをダウンロードします。
- 3 作成したディレクトリにキー ファイルを保存します。
- 4 ダウンロードする各キーに対して、以下のコマンドを実行してキーをインポートします。

```
# rpm --import /key_path/key_name
```

*key\_path* はキーを保存するディレクトリです。

*key\_name* は、キーのファイル名です。

## vCloud Director 用 NSX Data Center for vSphere のインストールと構成

vCloud Director インストールで NSX Data Center for vSphere からのネットワーク リソースを使用する場合は、NSX Data Center for vSphere をインストールして構成し、一意の NSX Manager インスタンスを vCloud Director インストールに含める各 vCenter Server インスタンスに関連付ける必要があります。

NSX Manager は NSX Data Center for vSphere ダウンロードに含まれています。vCloud Director と他の VMware 製品との互換性に関する最新情報については、[http://partnerweb.vmware.com/comp\\_guide/sim/interop\\_matrix.php](http://partnerweb.vmware.com/comp_guide/sim/interop_matrix.php) の「VMware 製品の相互運用性マトリックス」を参照してください。ネットワーク要件の詳細については、[vCloud Director のネットワーク構成要件](#)を参照してください。

---

**重要：** この手順は、vCloud Director の新規インストールを実行している場合のみ適用されます。vCloud Director の既存インストールをアップグレードしている場合は、[12 章 vCloud Director のアップグレード](#)を参照してください。

---

#### 前提条件

各 vCenter Server システムが NSX Manager をインストールするための前提条件を満たしていることを確認します。

#### 手順

- 1 NSX Manager 仮想アプライアンスのインストール タスクを実行します。  
『NSX インストール ガイド』を参照してください。
- 2 インストールした NSX Manager 仮想アプライアンスにログインし、インストール時に指定した設定を確認します。
- 3 インストールした NSX Manager 仮想アプライアンスを、vCloud Director インストールで vCloud Director に追加する vCenter Server システムに関連付けます。
- 4 関連付けられた NSX Manager インスタンスで VXLAN サポートを設定します。  
  
vCloud Director が VXLAN ネットワーク プールを作成し、プロバイダ VDC にネットワーク リソースを提供します。関連付けられた NSX Manager で VXLAN サポートが構成されていない場合は、プロバイダ VDC にネットワーク プール エラーが表示され、ユーザーが別のタイプのネットワーク プールを作成し、それをプロバイダ VDC に関連付ける必要があります。VXLAN サポートの構成に関する詳細については、『NSX 管理ガイド』を参照してください。
- 5 （オプション）システム内の Edge Gateway で分散ルーティングを実行する場合は、NSX Controller クラスタをセットアップします。  
  
『NSX 管理ガイド』を参照してください。

## vCloud Director 用 NSX-T Data Center のインストールと構成

vCloud Director インストールで NSX-T Data Center のネットワーク リソースを使用する場合は、NSX-T Data Center をインストールして設定する必要があります。

---

**重要：** NSX-T Data Center のオブジェクトおよびツールを設定するには、簡素化されたポリシー ユーザー インターフェイスと、簡素化されたユーザー インターフェイスに対応するポリシー API を使用します。詳細については、『NSX-T Data Center 管理ガイド』に記載されている NSX-T Manager の概要を参照してください。

---

vCloud Director と他の VMware 製品との互換性に関する最新情報については、[VMware 製品の相互運用性マトリックス](#)を参照してください。

ネットワーク要件の詳細については、[vCloud Director のネットワーク構成要件](#)を参照してください。

この手順は、vCloud Director の新規インストールを実行している場合のみ適用されます。vCloud Director の既存インストールをアップグレードしている場合は、[12 章 vCloud Director のアップグレード](#)を参照してください。

#### 前提条件

NSX-T Data Center について理解します。

#### 手順

- 1 NSX-T Manager 仮想アプライアンスをデプロイして設定します。

NSX-T Manager 環境の詳細については、NSX-T Data Center インストール ガイドを参照してください。

- 2 ネットワーク要件に基づいてトランスポート ゾーンを作成します。

トランスポート ゾーンの作成の詳細については、『NSX-T Data Center インストール ガイド』を参照してください。

---

#### 注：

---

- 3 Edge ノードと Edge クラスタをデプロイして設定します。

NSX Edge の作成の詳細については、『NSX-T Data Center インストール ガイド』を参照してください。

- 4 ESXi ホストのトランスポート ノードを設定します。

管理対象ホストのトランスポート ノードを設定する方法については、『NSX-T Data Center インストール ガイド』を参照してください。

- 5 Tier-0 ゲートウェイを作成します。

Tier-0 の作成の詳細については、『NSX-T Data Center 管理ガイド』を参照してください。

#### 次のステップ

vCloud Director をインストールすると、次のことが可能になります。

- 1 NSX-T Manager インスタンスのクラウドへの登録

NSX-T Manager インスタンスの登録の詳細については、『vCloud Director Service Provider Admin Portal Guide』を参照してください。

- 2 NSX-T Data Center トランスポート ゾーンによってバックアップされるネットワーク プールの作成

NSX-T Data Center トランスポート ゾーンによってバックアップされるネットワーク プールを作成する方法については、『vCloud Director Service Provider Admin Portal Guide』を参照してください。

- 3 Tier-0 ゲートウェイを外部ネットワークとしてインポート

NSX-T Data Center Tier-0 論理ルーターによってバックアップされている外部ネットワークを追加する方法については、『vCloud Director Service Provider Admin Portal Guide』を参照してください。

# Linux 上の vCloud Director 向けの SSL 証明書の作成と管理

# 4

vCloud Director では、クライアントとサーバ間で安全な通信を行うために SSL を使用します。各 vCloud Director サーバは、HTTPS 用とコンソール プロキシ通信用の 2 つの異なる SSL エンドポイントをサポートしている必要があります。

これらのエンドポイントには異なる IP アドレスを割り当てたり、同じ IP アドレスで 2 つの異なるポートを割り当てたりすることも可能です。各エンドポイントには独自の SSL 証明書が必要です。ワイルドカード証明書を使用するなど、両方のエンドポイントに同じ証明書を使用できます。

この章には、次のトピックが含まれています。

- [Linux 上の vCloud Director に SSL 証明書を作成する前に](#)
- [Linux 上での vCloud Director 用の自己署名付き SSL 証明書の作成](#)
- [Linux 上での vCloud Director 用の CA 署名付き SSL 証明書キーストアの作成](#)
- [Linux 上での vCloud Director 用にインポートされたプライベート キーを使用した、CA 署名付き SSL 証明書キーストアの作成](#)

## Linux 上の vCloud Director に SSL 証明書を作成する前に

vCloud Director for Linux をインストールするときに、サーバ グループのメンバーごとに 2 つの証明書を作成してホストのキーストアにインポートする必要があります。

---

**注：** サーバ グループ メンバーの証明書は、Linux に vCloud Director をインストールしてから作成する必要があります。vCloud Director アプライアンスによって、最初の起動時に自己署名 SSL 証明書が作成されます。

---

### 手順

1 vCloud Director サーバに root としてログインします。

2 サーバの IP アドレスを一覧表示します。

このサーバの IP アドレスを検出するには、`ifconfig` のようなコマンドを使用します。

3 IP アドレスごとに次のコマンドを実行して、IP アドレスの宛先となる完全修飾ドメイン名 (FQDN) を取得します。

```
nslookup ip-address
```



- 4 各 IP アドレスとそれに関連付けられた FQDN をメモしておきます。両方のサービスで単一の IP アドレスを使用していない場合は、HTTPS サービスの IP アドレスと、コンソール プロキシ サービスの IP アドレスを決定します。

証明書の作成時には FQDN を、ネットワークおよびデータベース接続の構成時には IP アドレスを指定する必要があります。IP アドレスにアクセスできるその他の FQDN をメモしておきます。証明書に Subject Alternative Names (SAN) を含める場合には指定する必要があるためです。

#### 次のステップ

2 台のエンドポイント用に証明書を作成します。信頼できる認証局 (CA) で署名された証明書か、自己署名証明書を使用できます。

---

**注：** CA 署名付き証明書は、最高レベルの信頼を提供します。

---

- CA 署名付き SSL 証明書の作成とインポートの詳細については、[Linux 上での vCloud Director 用の CA 署名付き SSL 証明書キーストアの作成](#)を参照してください。
- 自己署名 SSL 証明書の作成については、[Linux 上での vCloud Director 用の自己署名付き SSL 証明書の作成](#)を参照してください。
- 独自のプライベート キーおよび CA 署名付き証明書ファイルのインポートの詳細については、[Linux 上での vCloud Director 用にインポートされたプライベート キーを使用した、CA 署名付き SSL 証明書キーストアの作成](#)を参照してください。

## Linux 上での vCloud Director 用の自己署名付き SSL 証明書の作成

自己署名付き証明書は、信頼への懸念がごく小さい環境で vCloud Director の SSL を構成するのに便利な方法です。

各 vCloud Director サーバには、JCEKS キーストア ファイルに 2 つの SSL 証明書が必要です。1 つは HTTPS サービス用、もう 1 つはコンソール プロキシ サービス用です。

cell-management-tool を使用して、自己署名付きの SSL 証明書を作成します。インストール ファイルを実行してから設定エージェントを実行するまでの間に、cell-management-tool ユーティリティがセルにインストールされます。[サーバ グループの後続のメンバーへの vCloud Director のインストール](#)を参照してください。

---

**重要：** これらの例では 2048 ビットのキー サイズを指定しますが、適切なキー サイズを選択する前にインストールのセキュリティ要件を評価する必要があります。NIST Special Publication 800-131A に従い、1024 ビット未満のキー サイズはサポートされなくなりました。

---

#### 手順

- 1 vCloud Director サーバの OS に root として直接ログインするか、SSH クライアントを使用して接続します。

- 2 コマンドを実行して、HTTPS サービス用とコンソール プロキシ サービス用のパブリックおよびプライベート キー ペアを作成します。

```
/opt/vmware/vcloud-director/bin/cell-management-tool generate-certs -j -p -o certificates.ks -w passwd
```

このコマンドを実行すると、パスワードが passwd のキーストアが certificates.ks に作成されるか、更新されます。cell-management-tool は、コマンドのデフォルト値を使用して証明書を作成します。環境の DNS 構成に応じて、発行者の CN は各サービスの IP アドレスまたは FQDN に設定されます。証明書はキー長にデフォルトの 2048 ビットを使用し、作成後 1 年で期限切れになります。

---

**重要：** キーストア ファイルおよびキーストア ファイルが格納されているディレクトリは、ユーザー vcloud.vcloud から読み取り可能である必要があります。vCloud Director インストーラにより、このユーザーとグループが作成されます。

---

#### 次のステップ

キーストアのパス名をメモしておきます。構成スクリプトを実行して vCloud Director セルのネットワークとデータベース接続を作成するときに、キーストアのパス名が必要です。[ネットワークおよびデータベース接続の構成](#)を参照してください。

## Linux 上での vCloud Director 用の CA 署名付き SSL 証明書キーストアの作成

CA 署名付き証明書を作成およびインポートすると、SSL 通信の信頼レベルが最大になり、クラウド インフラストラクチャ内の接続を保護することができます。

各 vCloud Director サーバには、クライアントとサーバ間の通信を保護するために 2 つの SSL 証明書が必要です。各 vCloud Director サーバは、HTTPS 用とコンソール プロキシ通信用の 2 つの異なる SSL エンドポイントをサポートしている必要があります。

2 つのエンドポイントには異なる IP アドレスを割り当てたり、同じ IP アドレスで 2 つの異なるポートを割り当てたりすることも可能です。各エンドポイントには独自の SSL 証明書が必要です。ワイルドカード証明書を使用するなど、両方のエンドポイントに同じ証明書を使用できます。

いずれのエンドポイントの証明書にも、X.500 識別名と X.509 サブジェクトの別名拡張機能が含まれている必要があります。

信頼できる認証局 (CA) で署名された証明書か、自己署名証明書を使用できます。

cell-management-tool を使用して、自己署名付きの SSL 証明書を作成します。インストール ファイルを実行してから設定エージェントを実行するまでの間に、cell-management-tool ユーティリティがセルにインストールされます。[サーバ グループの後続のメンバーへの vCloud Director のインストール](#)を参照してください。

独自のプライベート キー ファイルと CA 署名付き証明書ファイルがすでに存在する場合は、[Linux 上での vCloud Director 用にインポートされたプライベート キー](#)を使用した、[CA 署名付き SSL 証明書キーストアの作成](#)に記載されている手順を実行します。

**重要：** これらの例では 2048 ビットのキー サイズを指定しますが、適切なキー サイズを選択する前にインストールのセキュリティ要件を評価する必要があります。NIST Special Publication 800-131A に従い、1024 ビット未満のキー サイズはサポートされなくなりました。

#### 前提条件

- `keytool` コマンドを使用して証明書をインポートできるように、Java バージョン 8 以降のランタイム環境のあるコンピュータにアクセスできることを確認します。vCloud Director インストーラでは `keytool` のコピーが `/opt/vmware/vcloud-director/jre/bin/keytool` に置かれますが、この手順は Java ランタイム環境がインストールされていればどのコンピュータでも実行できます。`keytool` で他のソースから作成された証明書を vCloud Director に使用することはできません。このコマンドラインの例では、`keytool` がユーザーのパス内にあることを前提としています。
- `keytool` コマンドについて理解しておきます。
- `generate-certs` コマンドで使用可能なオプションの詳細については、[HTTP およびコンソール プロキシ エンドポイントの自己署名証明書の生成](#)を参照してください。
- `certificates` コマンドで使用可能なオプションの詳細については、[HTTP およびコンソール プロキシ エンドポイントの証明書の置き換え](#)を参照してください。

#### 手順

- 1 vCloud Director サーバ セルの OS に `root` として直接ログインするか、SSH クライアントを使用して接続します。
- 2 コマンドを実行して、HTTPS サービス用とコンソール プロキシ サービス用のパブリックおよびプライベート キー ペアを作成します。

```
/opt/vmware/vcloud-director/bin/cell-management-tool generate-certs -j -p -o certificates.ks -w keystore_password
```

このコマンドを実行すると、キーストアが特定のパスワードで `certificates.ks` に作成されるか、更新されます。証明書はコマンドのデフォルト値を使用して作成されます。環境の DNS 構成に応じて、発行者の CN は各サービスの IP アドレスまたは FQDN に設定されます。証明書はキー長にデフォルトの 2048 ビットを使用し、作成後 1 年で期限切れになります。

**重要：** キーストア ファイルおよびキーファイルが格納されているディレクトリは、ユーザー `vcloud.vcloud` から読み取り可能である必要があります。vCloud Director インストーラにより、このユーザーとグループが作成されます。

### 3 HTTPS サービスとコンソール プロキシ サービスの証明書署名リクエストを作成します。

**重要：** HTTPS サービスとコンソール プロキシ サービスに異なる IP アドレスを使用している場合は、次のコマンドでホスト名と IP アドレスを調整します。

- a http.csr ファイル内に証明書署名リクエストを作成します。

```
keytool -keystore certificates.ks -storetype JCEKS -storepass keystore_password -certreq
-alias http -file http.csr -ext "san=dns:vcd2.example.com,dns:vcd2,ip:10.100.101.10"
```

- b consoleproxy.csr ファイル内に証明書署名リクエストを作成します。

```
keytool -keystore certificates.ks -storetype JCEKS -storepass keystore_password -certreq
-alias consoleproxy -file consoleproxy.csr -ext
"san=dns:vcd2.example.com,dns:vcd2,ip:10.100.101.10"
```

### 4 証明書署名リクエストを認証局に送信します。

証明書発行機関により、Web サーバー タイプを指定するよう求められる場合は、Jakarta Tomcat を使用します。

CA 署名付き証明書を取得します。

### 5 署名付き証明書を JCEKS キーストアにインポートします。

- a root.cer ファイルから certificates.ks キーストア ファイルに認証局のルート証明書をインポートします。

```
keytool -import -storetype JCEKS -storepass keystore_password -keystore certificates.ks
-alias root -file root_certificate_file
```

- b 中間証明書を受信した場合は、この証明書を intermediate.cer ファイルから certificates.ks キーストア ファイルにインポートします。

```
keytool -import -storetype JCEKS -storepass keystore_password -keystore certificates.ks
-alias intermediate -file intermediate_certificate_file
```

- c HTTPS サービス証明書をインポートします。

```
keytool -import -storetype JCEKS -storepass keystore_password -keystore certificates.ks
-alias http -file http_certificate_file
```

- d コンソール プロキシ サービスの証明書をインポートします。

```
keytool -import -storetype JCEKS -storepass keystore_password -keystore certificates.ks
-alias consoleproxy -file console_proxy_certificate_file
```

これらのコマンドは、certificates.ks ファイルを新しく取得した CA 署名付きバージョンの証明書で上書きします。

- 6 証明書が JCEKS キーストアにインポートされているかどうかを確認するには、次のコマンドを実行してキーストア ファイルの内容を一覧表示します。

```
keytool -storetype JCEKS -storepass keystore_password -keystore certificates.ks -list
```

- 7 サーバ グループ内のすべての vCloud Director サーバでこの手順を繰り返します。

#### 次のステップ

- vCloud Director インスタンスをまだ構成していない場合は、`configure` スクリプトを実行して証明書キーストアを vCloud Director にインポートします。 [ネットワークおよびデータベース接続の構成](#)を参照してください。

**注：** `certificates.ks` キーストア ファイルを作成したコンピュータが、完全修飾ドメイン名とそれに関連付けられた IP アドレスのリストを生成したサーバーとは異なる場合、ここでキーストア ファイルをそのサーバーにコピーします。構成スクリプトを実行するときに、キーストアのパス名が必要になります。

- vCloud Director インスタンスをすでにインストールして構成している場合は、セル管理ツールの `certificates` コマンドを使用して、証明書キーストアをインポートします。 [HTTP およびコンソール プロキシ エンドポイントの証明書の置き換え](#)を参照してください。

## Linux 上での vCloud Director 用にインポートされたプライベートキーを使用した、CA 署名付き SSL 証明書キーストアの作成

独自のプライベート キーおよび CA 署名付き証明書ファイルがある場合は、キーストアを vCloud Director 環境にインポートする前に、HTTPS サービスとコンソール プロキシ サービスの両方の証明書とプライベート キーをインポートするキーストア ファイルを作成する必要があります。

#### 前提条件

- [Linux 上の vCloud Director に SSL 証明書を作成する前に](#)を参照してください。
- `keytool` コマンドを使用して証明書をインポートできるように、Java バージョン 8 以降のランタイム環境のあるコンピュータにアクセスできることを確認します。vCloud Director インストーラでは `keytool` のコピーが `/opt/vmware/vcloud-director/jre/bin/keytool` に置かれますが、この手順は Java ランタイム環境がインストールされていればどのコンピュータでも実行できます。`keytool` で他のソースから作成された証明書を vCloud Director に使用することはできません。このコマンドラインの例では、`keytool` がユーザーのパス内にあることを前提としています。
- `keytool` コマンドについて理解しておきます。
- OpenSSL をダウンロードして、インストールします。
- `certificates` コマンドで使用可能なオプションの詳細については、[HTTP およびコンソール プロキシ エンドポイントの証明書の置き換え](#)を参照してください。

## 手順

- 1 中間証明書がある場合は、コマンドを実行してルート CA 署名証明書と中間証明書を結合し、証明書チェーンを作成します。

```
cat intermediate-certificate-file-1.cer intermediate-certificate-file-2.cer root-CA-certificate.cer > chain.crt
```

- 2 OpenSSL を使用して、HTTPS サービスとコンソール プロキシ サービスの両方のために、プライベート キー、証明書チェーン、それぞれのエイリアスを持つ中間 PKCS12 キーストア ファイルを作成し、各キーストア ファイルのパスワードを指定します。

- a HTTPS サービス用のキーストア ファイルを作成します。

```
openssl pkcs12 -export -in http.crt -inkey http.key -CAfile chain.crt -name http -passout pass:keystore_password -out http.pfx -chain
```

- b コンソール プロキシ サービス用のキーストア ファイルを作成します。

```
openssl pkcs12 -export -in consoleproxy.crt -inkey consoleproxy.key -CAfile chain.crt -name consoleproxy -passout pass:keystore_password -out consoleproxy.pfx -chain
```

- 3 keytool を使用して、PKCS12 キーストアを JCEKS キーストアにインポートします。

- a コマンドを実行して、HTTPS サービス用の PKCS12 キーストアをインポートします。

```
keytool -importkeystore -deststorepass keystore_password -destkeystore certificates.ks -deststoretype JCEKS -srckeystore http.pfx -srcstoretype PKCS12 -srcstorepass keystore_password
```

- b コマンドを実行して、コンソール プロキシ サービス用の PKCS12 キーストアをインポートします。

```
keytool -importkeystore -deststorepass keystore_password -destkeystore certificates.ks -deststoretype JCEKS -srckeystore consoleproxy.pfx -srcstoretype PKCS12 -srcstorepass keystore_password
```

- 4 証明書が JCEKS キーストアにインポートされているかどうかを確認するには、次のコマンドを実行してキーストア ファイルの内容を一覧表示します。

```
keytool -storetype JCEKS -storepass keystore_password -keystore certificates.ks -list
```

- 5 使用環境内のすべての vCloud Director セルに対してこの手順を繰り返します。

## 次のステップ

- vCloud Director インスタンスをまだ構成していない場合は、configure スクリプトを実行して証明書キーストアを vCloud Director にインポートします。 [ネットワークおよびデータベース接続の構成](#)を参照してください。

**注：** certificates.ks キーストア ファイルを作成したコンピュータが、完全修飾ドメイン名とそれに関連付けられた IP アドレスのリストを生成したサーバとは異なる場合は、キーストア ファイルをそのサーバにコピーします。構成スクリプトを実行するときに、キーストアのパス名が必要になります。

- vCloud Director インスタンスをすでにインストールして構成している場合は、セル管理ツールの `certificates` コマンドを使用して、証明書キーストアをインポートします。 [HTTP およびコンソール プロキシ エンドポイントの証明書の置き換え](#) を参照してください。

# Linux への vCloud Director のインストール

# 5

1 つ以上の Linux サーバの vCloud Director ソフトウェアをインストールすることで、vCloud Director サーバグループを作成できます。最初のグループ メンバーをインストールして構成すると、グループに追加メンバーを構成するときに使用する応答ファイルが作成されます。

この手順は、新しいインストールのみに適用します。既存の vCloud Director インストールをアップグレードする場合は、[12 章 vCloud Director のアップグレード](#)を参照してください。

---

**重要：** Linux 上の vCloud Director インストールおよび vCloud Director アプライアンス環境を 1 つのサーバグループ内で混在させることはできません。

---

## 前提条件

- サーバ グループのターゲット サーバが [2 章 vCloud Director のハードウェアおよびソフトウェア要件](#)を満たしていることを確認します。
- サーバ グループのターゲット サーバの各エンドポイントに対する SSL 証明書を作成したことを確認します。SSL 証明書へのパス名のすべてのディレクトリは、ユーザーから読み取り可能である必要があります。サーバグループのすべてのメンバーに、/tmp/certificates.ks などの同じキーストア パスを使用することで、インストール プロセスが簡素化されます。[Linux 上の vCloud Director に SSL 証明書を作成する前に](#)を参照してください。
- vCloud Director サーバ グループのすべてのターゲット サーバからアクセス可能な NFS またはその他の共有ストレージ ボリュームを準備していることを確認します。[転送サーバ ストレージの準備](#)を参照してください。
- グループ内のすべてのサーバからアクセス可能な vCloud Director データベースを作成したことを確認します。『[Linux での vCloud Director の外部 PostgreSQL データベースの構成](#)』を参照してください。データベース サーバを再起動するとデータベース サービスが開始することを確認します。
- すべての vCloud Director サーバ、データベース サーバ、すべての vCenter Server システム、および関連する NSX Manager インスタンスが、[vCloud Director のネットワーク構成要件](#)で説明されているように環境内の各ホスト名を解決できることを確認します。
- すべての vCloud Director サーバとデータベース サーバが、[vCloud Director のネットワーク構成要件](#)にある許容値の範囲内でネットワーク タイム サーバと同期していることを確認します。
- ユーザーまたはグループを LDAP サービスからインポートする予定がある場合、サービスが各 vCloud Director サーバにアクセスできることを確認します。



- [ネットワーク セキュリティの要件](#)に示されているように、ファイアウォール ポートを開きます。vCloud Director システムと vCenter Server システムの間でポート 443 が開いている必要があります。

## 手順

### 1 サーバ グループの後続のメンバーへの vCloud Director のインストール

環境を準備して前提条件を確認したら、最初のターゲットの Linux サーバで vCloud Director インストーラを実行して vCloud Director サーバ グループの作成を開始することができます。

### 2 ネットワークおよびデータベース接続の構成

サーバ グループの最初のメンバーに vCloud Director をインストールしたら、このセルのネットワーク接続とデータベース接続を作成する構成スクリプトを実行する必要があります。スクリプトは、サーバ グループに追加のメンバーを構成するときに使用する必要がある応答ファイルを作成します。

### 3 サーバ グループの後続のメンバーへの vCloud Director のインストール

vCloud Director サーバ グループにはいつでもサーバーを追加できます。サーバ グループのすべてのサーバは、同じデータベース接続の詳細を使用して構成する必要があるため、グループの最初のメンバーを構成したときに作成した応答ファイルを使用する必要があります。

## 次のステップ

サーバ グループのデータベースをシステム管理者のアカウントと関連情報で初期化するには、セル管理ツールの system-setup コマンドを使用します。『[vCloud Director インストール環境の構成](#)』を参照してください。

## サーバ グループの後続のメンバーへの vCloud Director のインストール

環境を準備して前提条件を確認したら、最初のターゲットの Linux サーバで vCloud Director インストーラを実行して vCloud Director サーバ グループの作成を開始することができます。

vCloud Director for Linux は、vmware-vcloud-director-distribution-v という形式の名前のデジタル署名された実行可能ファイルとして配布されます。v. v-nnnnnn.bin。ここで vv.v は、製品バージョン、nnnnnn はビルド番号を表します。例えば、vmware-vcloud-director-distribution-8.10.0-3698331.bin というファイル名になります。この実行可能ファイルを実行すると、vCloud Director がインストールまたはアップグレードされます。

vCloud Director インストーラでは、ターゲット サーバがプラットフォームのすべての前提条件を満たしていることを確認し、vCloud Director ソフトウェアをターゲット サーバにインストールします。

## 前提条件

- ターゲット サーバのスーパーユーザーの認証情報があることを確認します。
- インストーラにインストール ファイルのデジタル署名を検証させる場合、ターゲット サーバに VMware パブリック キーをダウンロードし、インストールします。インストール ファイルのデジタル署名をすでに検証している場合、インストール中にそれを再び検証する必要はありません。[VMware パブリック キーのダウンロードとインストール](#)を参照してください。

## 手順

- 1 ターゲット サーバに root としてログインします。

- 2 インストール ファイルをターゲット サーバーにダウンロードします。

メディアでソフトウェアを購入した場合は、ターゲット サーバからアクセス可能な場所にインストール ファイルをコピーします。

- 3 ダウンロード ページに投稿されているものとダウンロードのチェックサムが一致することを確認します。

MD5 と SHA1 チェックサムの値が、ダウンロード ページに投稿されます。適切なツールを使用して、ダウンロードされたインストール ファイルのチェックサムがダウンロード ページのものと一致することを確認します。次の形式の Linux コマンドは *installation-file* のチェックサムを表示します。

```
[root@cell1 /tmp]# md5sum installation-file
```

コマンドはインストール ファイルのチェックサムを返します。これは、ダウンロード ページの MD5 チェックサムと一致する必要があります。

- 4 インストール ファイルが実行可能であることを確認します。

インストール ファイルには実行権限が必要です。この権限を確実にインストール ファイルに設定するには、コンソール、シェル、またはターミナル ウィンドウを開き、次の Linux コマンドを実行します。*installation-file* は、vCloud Director インストール ファイルへのフル パス名です。

```
[root@cell1 /tmp]# chmod u+x installation-file
```

- 5 インストール ファイルを実行します。

インストール ファイルを実行するには、フル パス名を入力します。次に例を示します。

```
[root@cell1 /tmp]# ./installation-file
```

ファイルには、インストール スクリプトと組み込みの RPM パッケージが含まれます。

**注：** パス名に埋め込まれたスペース文字を含むディレクトリからインストール ファイルを実行することはできません。

ターゲット サーバに VMware パブリック キーをインストールしなかった場合、インストーラは次の形式の警告を出力します。

```
warning:installation-file.rpm: Header V3 RSA/SHA1 signature: NOKEY, key ID 66fd4949
```

インストーラは次のアクションを実行します。

- a ホストがすべての要件を満たすことを確認する。
- b インストール ファイルのデジタル署名を検証する。
- c vcloud ユーザーとグループを作成する。
- d vCloud Director RPM パッケージを展開する。
- e ソフトウェアをインストールする。

インストールが完了すると、インストーラにより、構成スクリプトを実行してネットワーク接続とデータベース接続を構成するよう求めるメッセージが表示されます。

## 6 構成スクリプトを実行するかどうかを選択します。

- a インタラクティブ モードで構成スクリプトを実行するには、**y** と入力して Enter を押します。
- b 後でインタラクティブ モードまたは無人モードで構成スクリプトを実行するには、**n** と入力して Enter を押します。

## ネットワークおよびデータベース接続の構成

サーバ グループの最初のメンバーに vCloud Director をインストールしたら、このセルのネットワーク接続とデータベース接続を作成する構成スクリプトを実行する必要があります。スクリプトは、サーバ グループに追加のメンバーを構成するときに使用する必要がある応答ファイルを作成します。

vCloud Director サーバ グループのすべてのメンバーは、データベース接続およびその他の構成の詳細を共有します。vCloud Director サーバ グループの最初のメンバーで構成スクリプトを実行すると、スクリプトは、以降のサーバ インストールで使用するデータベース接続情報を保持する応答ファイルを作成します。

構成スクリプトは、インタラクティブ モードまたは無人モードで実行できます。インタラクティブな構成の場合は、オプションなしでコマンドを実行し、スクリプトが必要な設定情報を求めるプロンプトを表示します。無人構成の場合は、コマンド オプションを使用して設定情報を指定します。

HTTP サービスとコンソール プロキシ サービスに対する 2 つの個別のポートを備えた 1 つの IP アドレスを使用する場合は、無人モードで構成スクリプトを実行する必要があります。

---

**注：** セル管理ツールには、最初に設定したネットワークおよびデータベース接続の詳細の変更に使用できるサブコマンドが含まれています。これらのサブコマンドを使用して実行した変更は、グローバル構成ファイルと応答ファイルに書き込まれます。セル管理ツールの使用については、「[10 章 セル管理ツール リファレンス](#)」を参照してください。

---

### 前提条件

- インタラクティブな構成の場合は、[インタラクティブな設定に関するリファレンス](#)を確認します。
- 無人構成の場合は、[無人構成のリファレンス](#)を確認します。
- 無人構成の場合は、VCLLOUD\_HOME 環境変数の値が vCloud Director のインストール先ディレクトリのフル パス名に設定されていることを確認してください。この値は通常、`/opt/vmware/vcloud-director` です。

### 手順

1 vCloud Director サーバに root としてログインします。

2 `configure` コマンドを実行します。

- インタラクティブ モードの場合は、コマンドを実行し、プロンプトに対して必要な情報を入力します。

```
/opt/vmware/vcloud-director/bin/configure
```

- 無人モードの場合は、適切なオプションと引数を指定してコマンドを実行します。

```
/opt/vmware/vcloud-director/bin/configure options -unattended
```

スクリプトは情報を検証し、次に以下を実行します。

- データベースを初期化し、サーバをデータベースに接続します。
- vCloud Director サービスが開始した後に [VMware vCloud Director のセットアップ] ウィザードに接続できる URL を表示します。
- vCloud Director セルを起動するよう指示します。

- 3 (オプション) [VMware vCloud Director のセットアップ] ウィザードの URL をメモし、**y** を入力して vCloud Director サービスを起動します。

`service vmware-vcd start` コマンドを実行して、後でサービスを起動することもできます。

## 結果

構成中に指定したデータベース接続情報とその他の再利用可能な情報は、このサーバの `/opt/vmware/vcloud-director/etc/responses.properties` にある応答ファイルに保存されます。このファイルには、サーバ グループにサーバを追加するときに再度使用する必要がある機密情報が含まれています。

## 次のステップ

応答ファイルのコピーを安全な場所に保存します。ファイルへのアクセスを制限し、必ず安全な場所にバックアップを作成します。ファイルのバックアップ時、公開ネットワークで平文を送信しないでください。

サーバをサーバ グループに追加する場合は、共有転送ストレージを `/opt/vmware/vcloud-director/data/transfer` にマウントします。

## インタラクティブな設定に関するリファレンス

インタラクティブ モードで `configure` スクリプトを実行すると、以下の情報を入力するようにスクリプトから求められます。

デフォルト値を受け入れる場合は、Enter キーを押します。

表 5-1. ネットワークおよびデータベースのインタラクティブな設定に必要な情報

必要な情報	説明
HTTP サービスの IP アドレス	デフォルトは、最初の使用可能な IP アドレスです。
コンソール プロキシ サービスの IP アドレス	デフォルトは、最初の使用可能な IP アドレスです。  <b>注：</b> HTTP サービスとコンソール プロキシ サービスに対する 2 つの個別のポートを備えた 1 つの IP アドレスを使用する場合は、無人モードで構成スクリプトを実行する必要があります。
Java キーストア ファイルのフル パス	例： <code>/opt/keystore/certificates.ks</code> 。
キーストアのパスワード	<a href="#">Linux 上の vCloud Director に SSL 証明書を作成する前に</a> を参照してください。

表 5-1. ネットワークおよびデータベースのインタラクティブな設定で必要な情報（続き）

必要な情報	説明
HTTP SSL 証明書のプライベート キーのパスワード	<a href="#">Linux 上の vCloud Director に SSL 証明書を作成する前に</a> を参照してください。
コンソール プロキシ SSL 証明書のプライベート キーのパスワード	<a href="#">Linux 上の vCloud Director に SSL 証明書を作成する前に</a> を参照してください。
Syslog ホストへのリモート監査ログ記録の有効化	<p>各 vCloud Director セル内のサービスは、監査メッセージを vCloud Director データベースにログとして記録し、メッセージは 90 日間保存されます。監査メッセージの保存期間を長くするには、監査メッセージを vCloud Director データベースだけでなく syslog ユーティリティに送信するように vCloud Director サービスを構成します。</p> <ul style="list-style-type: none"> <li>■ スキップする場合は、Enter キーを押します。</li> <li>■ 有効にする場合は、Syslog ホストの名または IP アドレスを入力します。</li> </ul>
リモート監査ログ記録を有効にした場合、Syslog ホストの UDP ポート	デフォルトは 514 です。
データベース サーバのホスト名または IP アドレス	データベースを実行しているサーバ。
データベース ポート	デフォルトは 5432 です。
データベース名	デフォルトは vcloud です。
データベース ユーザー名	『 <a href="#">Linux での vCloud Director の外部 PostgreSQL データベースの構成</a> 』を参照してください。
データベースのパスワード	『 <a href="#">Linux での vCloud Director の外部 PostgreSQL データベースの構成</a> 』を参照してください。
VMware カスタマ エクスペリエンス改善プログラム (CEIP) に参加する、または参加しない	<p>この製品は、VMware カスタマー エクスペリエンス向上プログラム（「CEIP」）に参加しています。CEIP を通じて収集されるデータについての詳細と、VMware がこの情報を使用する目的は、Trust &amp; Assurance Center (<a href="http://www.vmware.com/trustvmware/ceip.html">http://www.vmware.com/trustvmware/ceip.html</a>) で説明されています。セル管理ツールを使用して、この製品の VMware CEIP への参加または離脱をいつでも実行できます。『<a href="#">10 章 セル管理ツール リファレンス</a>』を参照してください。</p> <p>プログラムに参加する場合は、<b>y</b> と入力します。</p> <p>VMware の CEIP プログラムに参加しない場合は、<b>n</b> と入力します。</p>

## 無人構成のリファレンス

無人モードで configure スクリプトを実行する場合は、コマンド ラインで設定情報をオプションおよび引数として指定します。

表 5-2. 構成ユーティリティのオプションと引数

オプション	引数	説明
--help(-h)	なし	構成オプションと引数値のサマリを表示します。
--config-file (-c)	global.properties ファイルへのパス	構成ユーティリティを実行する時に指定した情報が、このファイルに保存されます。このオプションを省略すると、デフォルトの場所は /opt/vmware/vcloud-director/etc/global.properties になります。
--console-proxy-ip (-cons)	IPv4 アドレス。オプションでポート番号を付けることができます。	システムは、このアドレスを vCloud Director コンソール プロキシ サービスとして使用します。たとえば、10.17.118.159 とします。
--console-proxy-port-https	0~65535 の整数	vCloud Director コンソール プロキシ サービスが使用するポート番号。
--database-ssl	true または false	適切に署名された SSL 接続が vCloud Director から要求されるように、PostgreSQL データベースを設定できます。 PostgreSQL データベースで自己署名証明書またはプライベート証明書を使用する場合は、「 <a href="#">外部 PostgreSQL データベースでの追加設定の実行</a> 」を参照してください。
--database-host(-dbhost)	vCloud Director データベース ホストの IP アドレスまたは完全修飾ドメイン名	『 <a href="#">Linux での vCloud Director の外部 PostgreSQL データベースの構成</a> 』を参照してください。
--database-name (-dbname)	データベース サービス名	『 <a href="#">Linux での vCloud Director の外部 PostgreSQL データベースの構成</a> 』を参照してください。
--database-password (-dbpassword)	データベース ユーザーのパスワード。null にすることができます。	『 <a href="#">Linux での vCloud Director の外部 PostgreSQL データベースの構成</a> 』を参照してください。
--database-port (-dbport)	データベース ホスト上で動作するデータベース サービスによって使用されるポート番号	『 <a href="#">Linux での vCloud Director の外部 PostgreSQL データベースの構成</a> 』を参照してください。
--database-type (-dbtype)	データベース タイプ。サポートされているタイプは postgres です。	オプション。データベース タイプはデフォルトで postgres になります。『 <a href="#">Linux での vCloud Director の外部 PostgreSQL データベースの構成</a> 』を参照してください。
--database-user (-dbuser)	データベース ユーザーのユーザー名	『 <a href="#">Linux での vCloud Director の外部 PostgreSQL データベースの構成</a> 』を参照してください。

表 5-2. 構成ユーティリティのオプションと引数（続き）

オプション	引数	説明
--enable-ceip	true または false	この製品は、VMware カスタマー エクスペリエンス向上プログラム（「CEIP」）に参加しています。CEIP を通じて収集されるデータについての詳細と、VMware がこの情報を使用する目的は、Trust & Assurance Center ( <a href="http://www.vmware.com/trustvmware/ceip.html">http://www.vmware.com/trustvmware/ceip.html</a> ) で説明されています。セル管理ツールを使用して、この製品の VMware CEIP への参加または離脱をいつでも実行できます。『10 章 セル管理ツール リファレンス』を参照してください。
--uuid (-g)	なし	新規の一意のセル識別子を生成します
--primary-ip (-ip)	IPv4 アドレス。オプションでポート番号を付けることができます。	システムは、このアドレスを vCloud Director Web インターフェイス サービスに使用します。たとえば、10.17.118.159 とします。
--primary-port-http	0～65535 の整数	vCloud Director Web インターフェイス サービスへの HTTP（セキュリティ保護なし）接続に使用するポート番号
--primary-port-https	0～65535 の整数	vCloud Director Web インターフェイス サービスへの HTTPS（セキュリティ保護あり）接続に使用するポート番号
--keystore (-k)	SSL 証明書とプライベート キーが格納される Java キーストアへのパス	フル パス名を指定する必要があります。例：/opt/keystore/certificates.ks。
--syslog-host (-loghost)	syslog サーバ ホストの IP アドレスまたは完全修飾ドメイン名	各 vCloud Director セル内のサービスは、監査メッセージを vCloud Director データベースにログとして記録し、メッセージは 90 日間保存されます。監査メッセージの保存期間を長くするには、監査メッセージを vCloud Director データベースだけでなく syslog ユーティリティに送信するように vCloud Director サービスを構成します。
--syslog-port (-logport)	0～65535 の整数	指定したサーバを syslog プロセスが監視するポート。省略した場合のデフォルト値は 514 です。

表 5-2. 構成ユーティリティのオプションと引数（続き）

オプション	引数	説明
<code>--response-file (-r)</code>	応答ファイルへのパス	フル パス名を指定する必要があります。省略した場合のデフォルト値は、 <code>/opt/vmware/vcloud-director/etc/responses.properties</code> です。構成時に指定したすべての情報はこのファイルに保存されます。  <b>重要：</b> このファイルには、サーバ グループにサーバを追加するときに再度使用必要がある機密情報が含まれています。このファイルは安全な場所に保管し、必要な場合にのみ使用できるようにしてください。
<code>--unattended-installation (-unattended)</code>	なし	無人でのインストールを指定します。
<code>--keystore-password (-w)</code>	SSL 証明書キーストアのパスワード	SSL 証明書キーストアのパスワード。

### 例：2 つの IP アドレスを持つ無人構成

次のコマンド例は、HTTP サービスとコンソール プロキシ サービスに対する 2 つの個別の IP アドレスを使用する vCloud Director サーバの無人構成を実行します。

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./configure -ip 10.17.118.159 -cons 10.17.118.158 \
-dbtype postgres -dbhost 10.150.10.78 -dbname postgresql-db-name -dbuser vcloud --enable-ceip true \
-dbpassword P055word -k /opt/keystore/certificates.ks -w $3Cret -loghost 10.150.10.10 -unattended
```

### 例：1 つの IP アドレスを持つ無人構成

次のコマンド例は、HTTP サービスとコンソール プロキシ サービスに対する 2 つの個別のポートを備えた 1 つの IP アドレスを使用する vCloud Director サーバの無人構成を実行します。

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./configure -ip 10.17.118.159 --primary-port-https 9000 -cons 10.17.118.159 \
--console-proxy-port-https 9010 -dbtype postgres -dbhost 10.150.10.78 -dbname postgresql-db-name \
-dbuser vcloud -dbpassword P055word -k /opt/keystore/certificates.ks -w $3Cret \
-loghost 10.150.10.10 --enable-ceip true -unattended
```

## 応答ファイルの保護と再使用

最初の vCloud Director セルに構成したネットワークおよびデータベース接続の詳細は、応答ファイルに保存されます。このファイルには、サーバ グループにサーバを追加するときに再度使用必要がある機密情報が含まれています。このファイルは安全な場所に保管する必要があります。



応答ファイルは、最初にネットワークおよびデータベース接続を構成したサーバーの `/opt/vmware/vcloud-director/etc/responses.properties` に作成されます。グループにサーバを追加するときに、この応答ファイルのコピーを使用して、すべてのサーバで共有する構成パラメータを指定する必要があります。

**重要：** セル管理ツールには、最初に設定したネットワークおよびデータベース接続の詳細の変更に使用できるサブコマンドが含まれています。これらのツールを使用して行った変更内容はグローバル構成ファイルおよび応答ファイルに書き込まれるため、変更を可能にするコマンドを使用する前に応答ファイルが所定の場所 (`/opt/vmware/vcloud-director/etc/responses.properties`) に存在しており、書き込み可能であることを確認する必要があります。

## 手順

### 1 応答ファイルを保護します。

応答ファイルのコピーを安全な場所に保存します。ファイルへのアクセスを制限し、必ず安全な場所にバックアップを作成します。ファイルのバックアップ時、公開ネットワークで平文を送信しないでください。

### 2 応答ファイルを再使用します。

- a 構成の準備ができたサーバーからアクセスできる場所にファイルをコピーします。

**注：** 応答ファイルを再使用して構成する前に、サーバーに vCloud Director ソフトウェアをインストールする必要があります。応答ファイルのパス名にあるすべてのディレクトリは、次の例に示すように、ユーザー `vcloud.vcloud` から読み取り可能である必要があります。

```
[root@cell1 /tmp]# ls -l responses.properties
-rw----- 1 vcloud vcloud 418 Jun 8 13:42 responses.properties
```

インストーラにより、このユーザーとグループが作成されます。

- b `-r` オプションを使用し、応答ファイルのパス名を指定して、構成スクリプトを実行します。

`root` としてログインし、コンソール、シェル、またはターミナル ウィンドウを開き、次のように入力します。

```
[root@cell1 /tmp]# /opt/vmware/vcloud-director/bin/configure -r /path-to-response-file
```

## 次のステップ

追加のサーバーを構成したら、構成に使用した応答ファイルのコピーを削除します。

## サーバ グループの後続のメンバーへの vCloud Director のインストール

vCloud Director サーバ グループにはいつでもサーバーを追加できます。サーバ グループのすべてのサーバは、同じデータベース接続の詳細を使用して構成する必要があるため、グループの最初のメンバーを構成したときに作成した応答ファイルを使用する必要があります。

**重要：** Linux 上の vCloud Director インストールおよび vCloud Director アプライアンス環境を 1 つのサーバ グループ内で混在させることはできません。

### 前提条件

- このサーバ グループに最初のメンバーを構成したときに作成した応答ファイルにアクセスできることを確認します。[ネットワークおよびデータベース接続の構成](#)を参照してください。
- 共有転送ストレージを `/opt/vmware/vcloud-director/data/transfer` の vCloud Director サーバ グループの最初のメンバーにマウントしたことを確認します。

### 手順

- 1 ターゲット サーバに root としてログインします。

- 2 インストール ファイルをターゲット サーバにダウンロードします。

メディアでソフトウェアを購入した場合は、ターゲット サーバからアクセス可能な場所にインストール ファイルをコピーします。

- 3 インストール ファイルが実行可能であることを確認します。

インストール ファイルには実行権限が必要です。この権限を確実にインストール ファイルに設定するには、コンソール、シェル、またはターミナル ウィンドウを開き、次の Linux コマンドを実行します。*installation-file* は、vCloud Director インストール ファイルへのフル パス名です。

```
[root@cell1 /tmp]# chmod u+x installation-file
```

- 4 インストール ファイルを実行します。

インストール ファイルを実行するには、フル パス名を入力します。次に例を示します。

```
[root@cell1 /tmp]# ./installation-file
```

ファイルには、インストール スクリプトと組み込みの RPM パッケージが含まれます。

**注：** パス名に埋め込まれたスペース文字を含むディレクトリからインストール ファイルを実行することはできません。

ターゲット サーバに VMware パブリック キーをインストールしなかった場合、インストーラは次の形式の警告を出力します。

```
warning:installation-file.rpm: Header V3 RSA/SHA1 signature: NOKEY, key ID 66fd4949
```

インストーラは次のアクションを実行します。

- a ホストがすべての要件を満たすことを確認する。
- b インストール ファイルのデジタル署名を検証する。
- c vcloud ユーザーとグループを作成する。
- d vCloud Director RPM パッケージを展開する。
- e ソフトウェアをインストールする。

インストールが完了すると、インストーラにより、構成スクリプトを実行してネットワーク接続とデータベース接続を構成するよう求めるメッセージが表示されます。

- 5** **n** と入力し、Enter キーを押して構成スクリプトの実行を拒否します。

応答ファイルを入力として指定することによって、後で構成スクリプトを実行します。

- 6** `/opt/vmware/vcloud-director/data/transfer` に共有転送ストレージをマウントします。

サーバ グループのすべての vCloud Director サーバは、このボリュームを同じマウントポイントにマウントする必要があります。

- 7** このサーバからアクセスできる場所に応答ファイルをコピーします。

応答ファイルのパス名にあるすべてのディレクトリは、ルートから読み取り可能である必要があります。

- 8** 構成スクリプトを実行します。

- a 応答ファイルのパス名を指定して、`configure` コマンドを実行します。

```
/opt/vmware/vcloud-director/bin/configure -r /responses.properties
```

スクリプトは、応答ファイルを `vcloud.vcloud` で読み取り可能な場所にコピーし、応答ファイルを入力として使用して構成スクリプトを実行します。

- b プロンプトで、HTTP サービスおよびコンソール プロキシ サービスの IP アドレスを入力します。

- c 構成スクリプトが応答ファイルに保存されているパス名に有効な証明書を見つけられない場合は、プロンプトに対して証明書のパス名とパスワードを入力します。

スクリプトは情報を検証し、サーバをデータベースに接続して、vCloud Director セルを起動するように指示します。

- 9** (オプション) **y** と入力して vCloud Director サービスを起動します。

`service vmware-vcd start` コマンドを実行して、後でサービスを起動することもできます。

#### 次のステップ

このサーバ グループに他のサーバを追加するには、上記の手順を繰り返します。

vCloud Director サービスがすべてのサーバ上で稼働しているときに、vCloud Director データベースを、ライセンス キー、システム管理者アカウント、および関連情報で初期化する必要があります。セル管理ツールを使用してデータベースを初期化するには、`system-setup` サブコマンドを使用します。『[vCloud Director インストール環境の構成](#)』を参照してください。

# vCloud Director アプライアンスのデプロイ

# 6

vCloud Director アプライアンスの 1 つ以上のインスタンスをデプロイすることで、vCloud Director サーバグループを作成できます。vSphere Client (HTML5) または VMware OVF Tool を使用した vCloud Director アプライアンスをデプロイします。

**重要：** Linux 上の vCloud Director インストールおよび vCloud Director アプライアンス環境を 1 つのサーバグループ内で混在させることはできません。

vCloud Director アプライアンスは、vCloud Director サービスを実行するために最適化された、事前設定済みの仮想マシンです。

アプライアンスは、VMware vCloud Director-*v.v.v.v-nnnnnn\_OVF10.ova* という形式の名前で配布されます。ここで *vv.v.v* は、製品バージョン、*nnnnnn* はビルド番号を表します。例：VMware vCloud Director-9.7.0.0-9229800\_OVA10.ova

vCloud Director アプライアンスのパッケージには、次のソフトウェアが含まれています。

- VMware Photon™ OS
- vCloud Director サービス グループ
- PostgreSQL 10

ラボ システムまたはテスト システムに適している vCloud Director アプライアンスのサイズは、プライマリ（大）およびスタンバイ（小）です。プライマリ（大）およびスタンバイ（大）のサイズは、本番環境システムの最小のサイズ要件を満たします。ワークロードによっては、リソースの追加が必要になる場合があります。

**重要：** vCloud Director アプライアンスへのサードパーティ コンポーネントのインストールはサポートされていません。[VMware 製品の相互運用性マトリックス](#)に沿ってサポートされている VMware コンポーネントのみをインストールできます。たとえば、VMware vRealize® Operations Manager™ または VMware vRealize® Log Insight™ 監視エージェントをインストールできます。

## アプライアンス データベースの設定

バージョン 9.7 以降、vCloud Director アプライアンスには、高可用性 (HA) 機能を備えた組み込みの PostgreSQL データベースが含まれています。データベース HA クラスタを含むアプライアンス環境を作成するには、vCloud Director アプライアンスの 1 つのインスタンスをプライマリ セルとしてデプロイし、2 つのインスタンスをスタンバイ セルとしてデプロイする必要があります。vCloud Director アプライアンスの追加インスタンス

を vCD アプリケーション セルとしてサーバ グループにデプロイできます。このインスタンスでは、組み込みデータベースは使用せず、vCloud Director サービス グループのみが実行されます。vCD アプリケーション セルは、プライマリ セルのデータベースに接続されます。[アプライアンス環境とデータベースの高可用性構成](#)を参照してください。

デフォルトでは、vCloud Director アプライアンスは、レプリケーションなどのデータベース接続において、廃止された SSL の代わりに TLS を使用します。この機能は、自己署名 PostgreSQL 証明書を使用して、デプロイ後すぐにアクティブになります。認証局 (CA) からの署名付き証明書を使用するには、[自己署名の組み込み PostgreSQL および vCloud Director アプライアンスの管理ユーザー インターフェイス証明書の置き換え](#)を参照してください。

---

**注：** vCloud Director アプライアンスは、外部データベースをサポートしません。

---

## アプライアンス ネットワークの設定

バージョン 9.7 以降、データベース トラフィックから HTTP トラフィックを隔離するために vCloud Director アプライアンスは 2 つのネットワーク (eth0 と eth1) を使用してデプロイされます。複数のサービスが、対応するネットワーク インターフェイスのいずれかまたは両方で待機します。

---

**注：** eth0 ネットワークおよび eth1 ネットワークは、別のサブネットに配置する必要があります。

---

サービス	eth0 のポート	eth1 のポート
SSH	22	22
HTTP	80	該当なし
HTTPS	443	該当なし
PostgreSQL	該当なし	5432
管理ユーザー インターフェイス	5480	5480
コンソール プロキシ	8443	該当なし
JMX	8998、8999	該当なし
JMS/ActiveMQ	61616	該当なし

vCloud Director アプライアンスの作成後、vSphere ネットワーク機能を使用して、新しいネットワーク インターフェイス カード (NIC) を追加できます。『vSphere 仮想マシン管理』ガイドの[仮想マシンへのネットワーク アダプタの追加](#)情報を参照してください。

vCloud Director アプライアンスでは、ユーザーは iptables を使用してファイアウォール ルールをカスタマイズできます。カスタムの iptables ルールを追加するには、設定データを /etc/systemd/scripts/iptables ファイルの末尾に追加します。

この章には、次のトピックが含まれています。

- [アプライアンス環境とデータベースの高可用性構成](#)
- [vCloud Director アプライアンスのデプロイの前提条件](#)
- [vSphere Client を使用した vCloud Director アプライアンスのデプロイ](#)

## ■ VMware OVF Tool を使用した vCloud Director アプライアンスのデプロイ

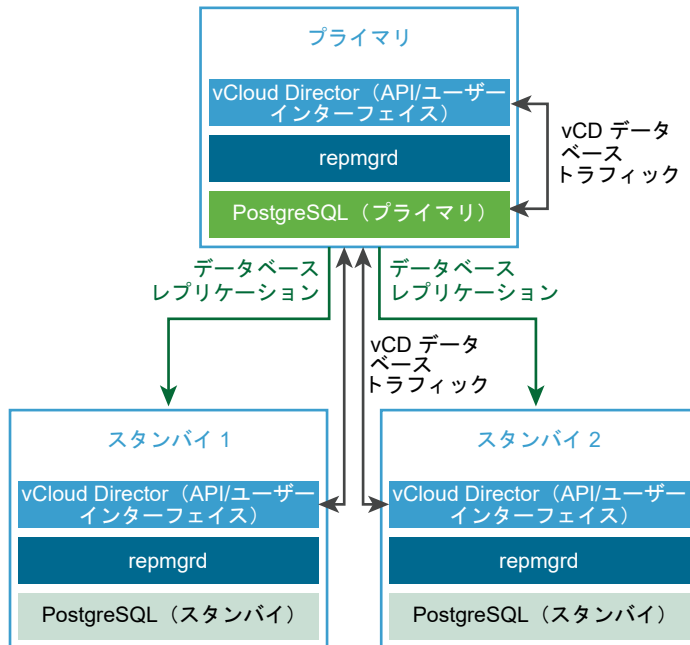
### アプライアンス環境とデータベースの高可用性構成

vCloud Director アプライアンスには、組み込みの PostgreSQL データベースが含まれています。組み込みの PostgreSQL データベースには、PostgreSQL サーバのクラスタに高可用性 (HA) 機能を提供する Replication Manager (repmgr) ツールスイートが含まれています。vCloud Director データベースにフェイルオーバー機能を提供するデータベース HA クラスタを使用して、アプライアンス環境を作成できます。

vCloud Director アプライアンスは、プライマリ セル、スタンバイ セル、または vCD アプリケーション セルとしてデプロイできます。 [vSphere Client を使用した vCloud Director アプライアンスのデプロイ](#)、[VMware OVF Tool を使用した vCloud Director アプライアンスのデプロイ](#)、または [HTTPS 通信およびコンソール プロキシ通信の署名付きワイルドカード証明書を使用した vCloud Director アプライアンスのデプロイ](#)を参照してください。

vCloud Director データベースに HA を構成するには、サーバ グループを作成するときに、vCloud Director アプライアンスのプライマリ インスタンスを 1 つ、スタンバイ インスタンスを 2 つデプロイして、データベース HA クラスタを構成します。

図 6-1. vCloud Director アプライアンス データベース HA クラスタ



### データベース HA 構成を含む vCloud Director アプライアンス環境の作成

データベース HA 構成を含む vCloud Director サーバ グループを作成するには、次のワークフローを実行します。

- 1 vCloud Director アプライアンスをプライマリ セルとしてデプロイします。

プライマリ セルは、vCloud Director サーバ グループの最初のメンバーです。組み込みデータベースは、vCloud Director データベースとして設定されます。データベース名は vcloud、データベース ユーザーは vcloud です。

## 2 プライマリ セルが実行中であることを確認します。

- a vCloud Director サービスの健全性を確認するには、システム管理者の認証情報を使用して、`https://primary_eth0_ip_address/provider` にある vCloud Director Service Provider Admin Portal にログインします。
- b PostgreSQL データベースの健全性を確認するには、`https://primary_eth1_ip_address:5480` にあるアプライアンス管理ユーザー インターフェイスに root としてログインします。

プライマリ ノードのステータスが実行中になっている必要があります。

## 3 vCloud Director アプライアンスの 2 つのインスタンスをスタンバイ セルとしてデプロイします。

組み込みデータベースは、プライマリ データベースを使用してレプリケーション モードで設定されます。

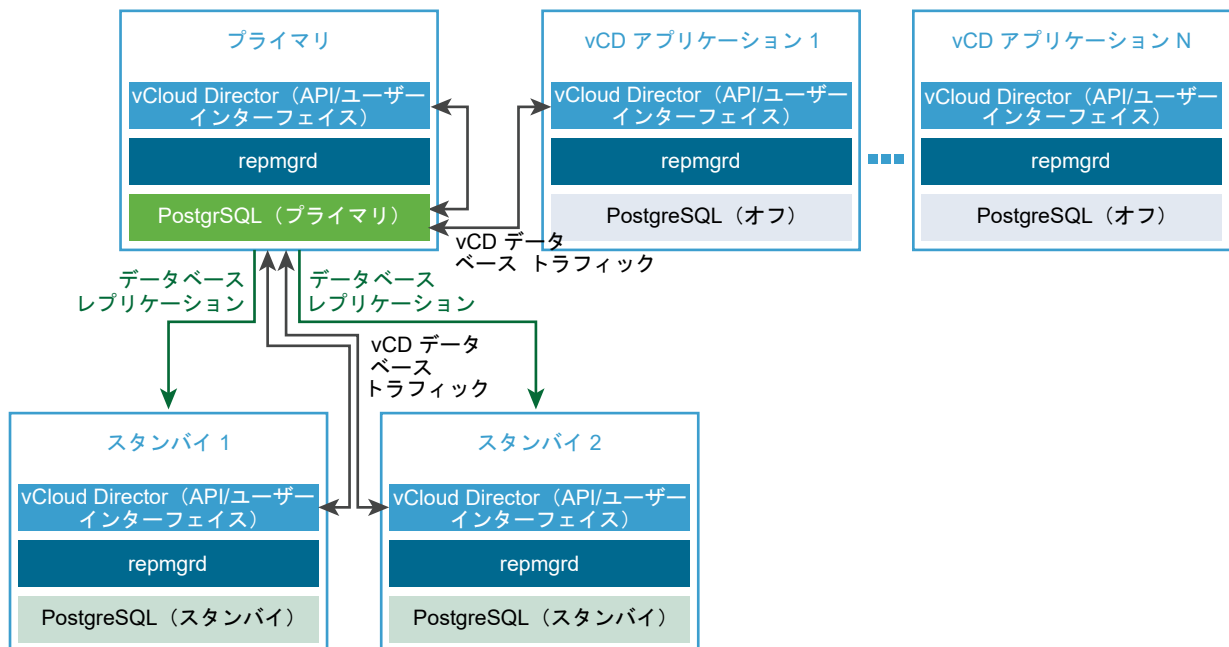
**注：** スタンバイ アプライアンスを最初にデプロイした後、Replication Manager はプライマリ アプライアンス データベースと自身のデータベースの同期を開始します。この期間中、vCloud Director データベースは使用できないため、vCloud Director のユーザー インターフェイスも使用できません。

## 4 HA クラスタ内のすべてのセルが実行中になっていることを確認します。

データベースの高可用性クラスタ内のセルのステータスの表示を参照してください。

## 5 (オプション) vCloud Director アプリケーション セルとして、vCloud Director アプライアンスのインスタンスを 1 つ以上デプロイします。

組み込みデータベースは使用されません。vCloud Director アプリケーション セルは、プライマリ データベースに接続されます。



## データベース HA 構成を含まない vCloud Director アプライアンス環境の作成

**注：** 1つのプライマリ セルを持ち、スタンバイ セルまたはアプリケーション セルを持たない、vCloud Director クラスターをデプロイできます。単一セルのデプロイ環境は、データベースの観点から単一障害点であるため、VMware は、本番環境での単一セルのデプロイにはサポートを提供しません。単一セルのデプロイ環境の場合、パフォーマンスや安定性に関連する問題はサポート対象外です。

データベース HA 構成を含まない vCloud Director サーバを作成するには、次のワークフローを実行します。

- 1 vCloud Director アプライアンスをプライマリ セルとしてデプロイします。

プライマリ セルは、vCloud Director サーバ グループの最初のメンバーです。組み込みデータベースは、vCloud Director データベースとして設定されます。データベース名は vcloud、データベース ユーザーは vcloud です。

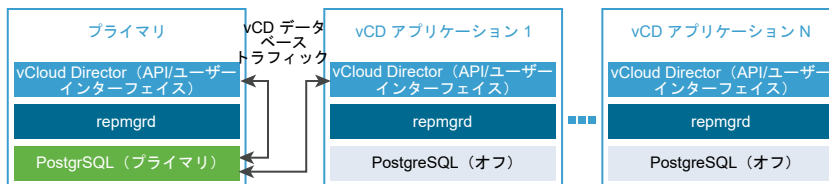
- 2 プライマリ セルが実行中であることを確認します。

- a vCloud Director サービスの健全性を確認するには、システム管理者の認証情報を使用して、`https://primary_eth0_ip_address/provider` にある vCloud Director Service Provider Admin Portal にログインします。
- b PostgreSQL データベースの健全性を確認するには、`https://primary_eth1_ip_address:5480` にあるアプライアンス管理ユーザー インターフェイスに root としてログインします。

プライマリ ノードのステータスが実行中になっている必要があります。

- 3 (オプション) vCD アプリケーション セルとして、vCloud Director アプライアンスのインスタンスを 1 つ以上デプロイします。

組み込みデータベースは使用されません。vCD アプリケーション セルは、プライマリ データベースに接続されます。



## vCloud Director アプライアンスのデプロイの前提条件

vCloud Director アプライアンスのデプロイを成功させるには、デプロイを開始する前にいくつかのタスクと事前チェックを実行する必要があります。

- vCloud Director の .ova ファイルにアクセスできることを確認します。



- プライマリ アプライアンスをデプロイする前に、NFS 共有転送サービスのストレージを準備します。[転送サーバストレージの準備](#)を参照してください。

---

**注：** 共有転送サービスのストレージには、responses.properties ファイルも appliance-nodes ディレクトリも含めないでください。

---

- [RabbitMQ AMQP ブローカのインストールおよび構成](#)。

## vCloud Director アプライアンスのデプロイ方法

- [vSphere Client を使用した vCloud Director アプライアンスのデプロイ](#)
- [VMware OVF Tool を使用した vCloud Director アプライアンスのデプロイ](#)
- [HTTPS 通信およびコンソール プロキシ通信の署名付きワイルドカード証明書を使用した vCloud Director アプライアンスのデプロイ](#)

## vSphere Client を使用した vCloud Director アプライアンスのデプロイ

vSphere Client (HTML5) を使用して、vCloud Director アプライアンスを OVF テンプレートとしてデプロイできます。

vCloud Director サーバ グループの最初のメンバーはプライマリ セルとしてデプロイする必要があります。vCloud Director サーバ グループの後続のメンバーは、スタンバイ セルまたは vCD アプリケーション セルとしてデプロイできます。[アプライアンス環境とデータベースの高可用性構成](#)を参照してください。

---

**重要：** Linux 上の vCloud Director インストールおよび vCloud Director アプライアンス環境を 1 つのサーバグループ内で混在させることはできません。

追加または置き換えのアプライアンスをデータベース クラスタに追加する場合、vCPU および RAM はクラスタ内の既存のプライマリ セルとスタンバイ セルのものと一致させる必要があります。

新しくデプロイされたスタンバイの OVA のバージョンは、クラスタ内の既存のアプライアンスと同じである必要があります。実行中のアプライアンスのバージョンを確認するには、アプライアンス管理ユーザー インターフェイスのバージョン情報を表示します。アプライアンスは、VMware Cloud Director-v.v.v.v-*nnnnnn*\_OVF10.ova という形式の名前で配布されます。ここで v.v.v.v は、製品バージョン、*nnnnnn* はビルド番号を表します。例：  
VMware Cloud Director-10.0.0.0-9229800\_OVA10.ova

---

vSphere に OVF テンプレートをデプロイする方法の詳細については、「vSphere 仮想マシン管理」を参照してください。

別の方法として、VMware OVF Tool を使用してアプライアンスをデプロイすることもできます。[VMware OVF Tool を使用した vCloud Director アプライアンスのデプロイ](#)を参照してください。

---

**注：** vCloud Director への vCloud Director アプライアンスのデプロイはサポートされていません。

---

## 前提条件

[vCloud Director アプライアンスのデプロイの前提条件](#)を参照してください。

## 手順

### 1 vCloud Director アプライアンスのサイジング ガイドライン

必要に応じて、vCloud Director アプライアンス ベースのサーバ グループに個別の構成を使用したり、vCloud Director 仮想アプライアンス インスタンスに異なるサイズを使用したりできます。

### 2 vCloud Director アプライアンスのデプロイの開始

アプライアンスのデプロイを開始するには、vSphere Web Client (Flex) または vSphere Client (HTML5) からデプロイ ウィザードを開きます。

### 3 vCloud Director アプライアンスのカスタマイズとデプロの終了

vCloud Director の詳細を構成するには、アプライアンス テンプレートをカスタマイズします。

## 次のステップ

- vCloud Director アプライアンスはコンソール プロキシ サービスに eth0 NIC とカスタム ポート 8443 を使用するため、公開コンソールのプロキシ アドレスを構成します。[公開アドレスのカスタマイズ](#)を参照してください。
- vCloud Director サーバ グループにメンバーを追加するには、手順を繰り返します。
- ライセンス キーを入力するには、vCloud Director Service Provider Admin Portal にログインします。
- アプライアンスの最初の起動時に作成された自己署名証明書を置き換えるには、[Linux 上での vCloud Director 用の CA 署名付き SSL 証明書キーストアの作成](#)ができます。

## vCloud Director アプライアンスのサイジング ガイドライン

必要に応じて、vCloud Director アプライアンス ベースのサーバ グループに個別の構成を使用したり、vCloud Director 仮想アプライアンス インスタンスに異なるサイズを使用したりできます。

## 概要

プライマリ セルで障害が発生した場合にクラスタが自動フェイルオーバーをサポートできるように、vCloud Director の最小デプロイは 1 つのプライマリ セルと 2 つのスタンバイ セルで構成される必要があります。この環境は、何らかの理由でいずれかのセルがオフラインになる障害シナリオでも引き続き利用できます。スタンバイ障害が発生した場合、障害が発生したセルを再デプロイするまで、クラスタはパフォーマンスをいくらか低下させながら完全に機能した状態で動作します。[アプライアンス環境とデータベースの高可用性構成](#)を参照してください。

vCloud Director アプライアンスには、デプロイ時に選択できる 4 つのサイズ（小、中、大、特大 (VVD)）があります。小規模アプライアンス サイズはラボの評価に適しています。このドキュメントでは、小規模アプライアンス 構成に関するガイダンスは提供していません。サイジング オプションの表に、その他のオプションの仕様と、本番環境に最適な使用事例を示します。特大構成は、[VMware Validated Designs \(VVD\) for Cloud Providers](#) のスケール プロファイルと一致しています。

より大きなカスタム サイズを作成するために、システム管理者はデプロイされたセルのサイズを調整できます。

本番環境で推奨される最小の構成は、中規模仮想アプライアンスの 3 ノードによるデプロイです。

**注：** 1つのプライマリ セルを持ち、スタンバイ セルまたはアプリケーション セルを持たない、vCloud Director クラスタをデプロイできます。単一セルのデプロイ環境は、データベースの観点から単一障害点であるため、VMware は、本番環境での単一セルのデプロイにはサポートを提供しません。単一セルのデプロイ環境の場合、パフォーマンスや安定性に関連する問題はサポート対象外です。

## vCloud Director アプライアンスのサイジング オプション

次の決定ガイドを使用して、環境のアプライアンス サイズを見積もることができます。

	中	大	特大 (VVD)
推奨される使用事例	ラボ環境または小規模な本番環境	本番環境	API 統合および監視を使用する本番環境
vRealize Operations Management Pack 環境での vCloud Director のデプロイ	いいえ	いいえ	はい
vCloud Director での Cassandra 仮想マシン メトリックの有効化	いいえ	いいえ	はい
30 分のピーク期間に API にアクセスする同時実行ユーザーまたはクライアントの概数。	< 50	< 100	< 100
管理対象仮想マシン	5,000	5,000	15,000

## 構成の定義

**注：** vCloud Director 9.7 以降の primary-large および standby-large アプライアンスには、デフォルトで、大規模 HA クラスタ構成に必要な 16 個の vCPU が設定されていません。大規模な vCloud Director アプライアンス構成を使用する場合は、デプロイ後にプライマリ セルとスタンバイ セルの vCPU を手動で 16 に変更する必要があります。

	中	大	特大 (VVD)
HA クラスタ構成	1つのプライマリ セル + 2つのスタンバイ セル	1つのプライマリ セル + 2つのスタンバイ セル + 1つのアプリケーション セル	1つのプライマリ セル + 2つのスタンバイ セル + 2つのアプリケーション セル
vCPU のプライマリ セルまたはスタンバイ セル	8	16	24
vCPU アプリケーション セル	該当なし	8	8
RAM プライマリ セルまたはスタンバイ セル	16 GB	24 GB	32 GB
RAM アプリケーション セル	該当なし	8	8

	中	大	特大 (VVD)
vCPU と物理コアの比率	1:1	1:1	1:1
プライマリ セルとスタンバイ セルでの PostgreSQL のカスタマイズ	shared_buffers = '3GB'; effective_cache_size = '9GB'; work_mem = '8MB'; maintenance_work_mem = '1GB'; max_worker_processes= '8';	shared_buffers = '5GB'; effective_cache_size = '15GB'; work_mem = '8MB'; maintenance_work_mem = '1GB'; max_worker_processes= '16';	shared_buffers = '7GB'; effective_cache_size = '21GB'; work_mem = '8MB'; maintenance_work_mem = '1GB'; max_worker_processes= '24';

## システムがサイズ不足かどうかを検出する方法

vCloud Director セルでは、CPU またはメモリの使用量が増加すると、高レベル、つまりキャパシティ近くのレベルで推移します。また、vCloud Director セルでデータベースへの接続が切断されることがあります。

## システムのセル数が不十分かどうかを検出する方法

いずれかの vCloud Director セルの vcloud-container-debug.log および cell-runtime.log ファイルに以下のようなエントリが記録されます：org.apache.tomcat.jdbc.pool.PoolExhaustedException: [pool-jetty-XXXXX] Timeout: Pool empty.Unable to fetch a connection in 20 seconds, none available。また、vCloud Director セルでデータベースへの接続が切断されることがあります。

**注：** デフォルトのデータベース接続構成に基づいて、すべての構成は、プライマリ、スタンバイ、アプリケーション タイプで最大 6 セルに制限されます。

## アプライアンスのサイジングをカスタマイズする方法

vCloud Director アプライアンスのサイジングをサポートされている構成のいずれかにカスタマイズするには、vCloud Director アプライアンス デプロイの実行後、すべてのセルで次の手順を実行する必要があります。

- 1 選択した構成に必要な数のセルがあることを確認します。
- 2 すべてのセルのメモリと vCPU を、サポートされている構成のいずれかに一致するように調整します。

**重要：** RAM と vCPU の容量は、すべてのプライマリ セルとスタンバイ セルで同じである必要があります。

- 3 プライマリ アプライアンスの OS に root として直接ログインするか、SSH クライアントを使用して接続します。
- 4 ユーザーを postgres に変更します。

```
sudo -i -u postgres
```

- 5 次のコマンドを実行して、`postgresql.auto.conf` 構成ファイルを更新します。

構成タイプ	説明
中	<pre>psql -c "ALTER SYSTEM set shared_buffers = '3GB';" psql -c "ALTER SYSTEM set effective_cache_size = '9GB';" psql -c "ALTER SYSTEM set work_mem = '8MB';" psql -c "ALTER SYSTEM set maintenance_work_mem = '1GB';" psql -c "ALTER SYSTEM set max_worker_processes= '8';"</pre>
大	<pre>psql -c "ALTER SYSTEM set shared_buffers = '5GB';" psql -c "ALTER SYSTEM set effective_cache_size = '15GB';" psql -c "ALTER SYSTEM set work_mem = '8MB';" psql -c "ALTER SYSTEM set maintenance_work_mem = '1GB';" psql -c "ALTER SYSTEM set max_worker_processes= '16';"</pre>
特大	<pre>psql -c "ALTER SYSTEM set shared_buffers = '7GB';" psql -c "ALTER SYSTEM set effective_cache_size = '21GB';" psql -c "ALTER SYSTEM set work_mem = '8MB';" psql -c "ALTER SYSTEM set maintenance_work_mem = '1GB';" psql -c "ALTER SYSTEM set max_worker_processes= '24';"</pre>

- 6 `exit` コマンドを実行して root ユーザーに戻ります。

- 7 `vpostgres` プロセスを再開します。

```
systemctl restart vpostgres
```

- 8 ユーザーを `postgres` に再度変更します。

```
sudo -i -u postgres
```

- 9 各スタンバイ ノードで、`postgresql.auto.conf` ファイルをノードにコピーし、`vpostgres` プロセスを再開します。

- a `postgresql.auto.conf` をプライマリ ノードからスタンバイ ノードにコピーします。

```
scp /var/vmware/vpostgres/current/pgdata/postgresql.auto.conf postgres@<standby-node-address>:/var/vmware/vpostgres/current/pgdata/
```

- b `vpostgres` プロセスを再開します。

```
systemctl restart vpostgres
```

vCloud Director アプライアンスのサイジングをカスタム構成にカスタマイズするには、vCloud Director アプライアンス デプロイの実行後、すべてのセルで次の手順を実行する必要があります。

- 1 プライマリ アプライアンスの OS に root として直接ログインするか、SSH クライアントを使用して接続します。
- 2 vCPU 情報を表示してメモするには、次のコマンドを実行します。

```
grep -c processor /proc/cpuinfo
```

- 3 RAM 情報を表示してメモするには、次のコマンドを実行します。

以下で報告されている RAM は KB 単位であるため、1,024,000 で割って GB に変換する必要があります。

```
cat /proc/meminfo | grep MemTotal | cut -dk -f1 | awk '{print int($2/1024000)}'
```

- 4 shared\_buffers の値は、RAM の合計から 4 GB を引き、1/4 倍して計算します。

$\text{shared\_buffers} = 0.25 * (\text{total RAM} - 4\text{GB})$

- 5 effective\_cache\_size の値は、RAM の合計から 4 GB を引き、3/4 倍して計算します。

$\text{effective\_cache\_size} = 0.75 * (\text{total RAM} - 4\text{GB})$

- 6 max\_worker\_processes の値は vCPU の数として計算します。

- 7 ユーザーを postgres に変更します。

```
sudo -i -u postgres
```

- 8 次のコマンドを実行し、計算した値に置き換えて Postgresql.auto.conf 構成ファイルを更新します。

```
psql -c "ALTER SYSTEM set shared_buffers = 'shared_buffers value';"
psql -c "ALTER SYSTEM set effective_cache_size = 'effective_cache_size value';"
psql -c "ALTER SYSTEM set work_mem = '8MB';"
psql -c "ALTER SYSTEM set maintenance_work_mem = '1GB';"
psql -c "ALTER SYSTEM set max_worker_processes= 'max_worker_processes value';"
```

- 9 exit コマンドを実行して root ユーザーに戻ります。

- 10 vpostgres プロセスを再開します。

```
systemctl restart vpostgres
```

- 11 ユーザーを postgres に再度変更します。

```
sudo -i -u postgres
```

- 12 各スタンバイ ノードで、`postgresql.auto.conf` ファイルをノードにコピーし、`vpostgres` プロセスを再開します。

- a `postgresql.auto.conf` をプライマリ ノードからスタンバイ ノードにコピーします。

```
scp /var/vmware/vpostgres/current/pgdata/postgresql.auto.conf postgres@standby-node-  
address:/var/vmware/vpostgres/current/pgdata/
```

- b `vpostgres` プロセスを再開します。

```
systemctl restart vpostgres
```

## vCloud Director アプライアンスのデプロイの開始

アプライアンスのデプロイを開始するには、vSphere Web Client (Flex) または vSphere Client (HTML5) からデプロイ ウィザードを開きます。

### 手順

- 1 vSphere Web Client または vSphere Client でインベントリ オブジェクトを右クリックし、[OVF テンプレートのデプロイ] をクリックします。
- 2 vCloud Director の `.ova` ファイルのパスを入力し、[次へ] をクリックします。
- 3 仮想マシンの名前を入力し、vCenter Server リポジトリを参照して、アプライアンスをデプロイするデータセンターまたはフォルダを選択し、[次へ] をクリックします。
- 4 アプライアンスをデプロイする ESXi ホストまたはクラスタを選択し、[次へ] をクリックします。
- 5 テンプレートの詳細を確認し、[次へ] をクリックします。
- 6 使用許諾契約書を読んで同意し、[次へ] をクリックします。
- 7 デプロイのタイプおよびサイズを選択して、[次へ] をクリックします。

ラボ システムまたはテスト システムに適している vCloud Director アプライアンスのサイズは、プライマリ (大) およびスタンバイ (小) です。プライマリ (大) およびスタンバイ (大) のサイズは、本番環境システムの最小のサイズ要件を満たします。ワークロードによっては、リソースの追加が必要になる場合があります。

オプション	説明
プライマリ (小)	12 GB の RAM と 2 つの vCPU を搭載したアプライアンスを、vCloud Director サーバグループの最初のメンバーとしてデプロイします。  プライマリ セルの組み込みデータベースは、vCloud Director データベースとして設定されます。データベース名は <code>vccloud</code> 、データベース ユーザーは <code>vccloud</code> です。
プライマリ (大)	24 GB の RAM と 4 つの vCPU を搭載したアプライアンスを、vCloud Director サーバグループの最初のメンバーとしてデプロイします。  プライマリ セルの組み込みデータベースは、vCloud Director データベースとして設定されます。データベース名は <code>vccloud</code> 、データベース ユーザーは <code>vccloud</code> です。

オプション	説明
スタンバイ (小)	<p>データベース HA クラスタにプライマリ (小) セルを追加する場合に使用します。</p> <p>12 GB の RAM と 2 つの vCPU を搭載したアプライアンスを、データベース高可用性構成の vCloud Director サーバ グループの 2 番目または 3 番目のメンバーとしてデプロイします。</p> <p>スタンバイ セルの組み込みデータベースは、プライマリ データベースを使用してレプリケーション モードで設定されます。</p>
スタンバイ (大)	<p>データベース HA クラスタにプライマリ (大) セルを追加する場合に使用します。</p> <p>24 GB の RAM と 4 つの vCPU を搭載したアプライアンスを、データベース高可用性構成の vCloud Director サーバ グループの 2 番目または 3 番目のメンバーとしてデプロイします。</p> <p>スタンバイ アプライアンスの組み込みデータベースは、プライマリ データベースを使用してレプリケーション モードで設定されます。</p>
vCD セル アプリケーション	<p>8 GB の RAM と 2 つの vCPU を搭載したアプライアンスを、vCloud Director サーバ グループの後続のメンバーとしてデプロイします。</p> <p>vCD アプリケーション セル内の組み込みデータベースは使用されません。vCD アプリケーション セルは、プライマリ データベースに接続されます。</p>

**重要：** vCloud Director サーバ グループ内のプライマリ セルおよびスタンバイ セルは、同じサイズである必要があります。データベース HA クラスタは、1 つのプライマリ セル (小) と 2 つのスタンバイ セル (小)、または 1 つのプライマリ セル (大) と 2 つのスタンバイ セル (大) で構成できます。

デプロイ後に、アプライアンスのサイズを再設定できます。

- 8 仮想マシン構成ファイルと仮想ディスクのディスク フォーマットとデータストアを選択し、[次へ] をクリックします。

シック フォーマットはパフォーマンスを向上させ、シン フォーマットはストレージ容量を節約します。

- 9 [ターゲット ネットワーク] セルのドロップダウン メニューから、アプライアンスの eth1 NIC および eth0 NIC のターゲット ネットワークを選択します。

**重要：** 2 つのターゲット ネットワークは異なっている必要があります。

- 10 [IP アドレスの割り当て設定] ドロップダウン メニューから [固定 - 手動] IP 割り当てを選択して、[IPv4] プロトコルを選択します。

- 11 [次へ] をクリックします。

vCloud Director の詳細を設定する [テンプレートのカスタマイズ] 画面にリダイレクトされます。

## vCloud Director アプライアンスのカスタマイズとデプロの終了

vCloud Director の詳細を構成するには、アプライアンス テンプレートをカスタマイズします。



vCloud Director アプライアンスをカスタマイズする場合は、アプライアンスの設定、データベース、およびネットワークのプロパティを設定します。システムの初期設定は、サーバ グループの最初のメンバーであるプライマリ アプライアンスをデプロイする場合のみ行います。

**注：** この手順の**手順 3** のみがオプションです。vCloud Director アプライアンスをカスタマイズするには、その他のすべての手順を完了する必要があります。

## 手順

- 1 [VCD アプライアンス設定] セクションで、アプライアンスの詳細を設定します。

設定	説明
NTP サーバ	使用する NTP サーバのホスト名または IP アドレスです。
初期の root パスワード	<p>アプライアンスの初期 root パスワード。8 文字以上（大文字、小文字、数字、特殊文字をそれぞれ 1 文字以上）を含める必要があります。</p> <p><b>重要：</b> 初期の root パスワードがキーストアのパスワードになります。クラスタ環境では、初期導入時にすべてのセルに同じ root パスワードを設定する必要があります。起動プロセスが完了したら、目的の任意のセルの root パスワードを変更できます。</p> <p><b>注：</b> OVF デプロイ ウィザードは、パスワードの基準に対して初期 root パスワードを検証しません。</p>
最初のログイン時に root パスワードを期限切れにする	最初のログイン後も初期パスワードを引き続き使用する場合は、初期パスワードが root パスワードの基準を満たしていることを確認する必要があります。最初のログイン後も初期 root パスワードを引き続き使用するには、このオプションを選択解除します。
SSH の有効化	デフォルトでは無効です。
転送ファイルの場所への NFS マウント	<a href="#">転送サーバストレージの準備</a> を参照してください。

**注：** アプライアンスの日付、時刻、タイム ゾーンの変更については、[「https://kb.vmware.com/kb/59674」](https://kb.vmware.com/kb/59674)を参照してください。

- 2 サーバ グループの最初のメンバーをデプロイする場合は、[VCD の設定 - 「プライマリ」 アプライアンスの場合のみ必要] セクションにデータベースの詳細を入力し、システム管理者アカウントを作成して、システム設定を行います。

データベース名は vcloud、データベース ユーザーは vcloud です。

設定	説明
「vcloud」ユーザーの「vcloud」データベースパスワード	vcloud データベース ユーザーのパスワード。
管理ユーザー名	システム管理者アカウントのユーザー名。デフォルトでは administrator です。
管理者の完全な名前	システム管理者の完全な名前。デフォルトでは vCD Admin です。
管理者ユーザーのパスワード	システム管理者アカウントのパスワード。
管理者の E メール	システム管理者のメール アドレス。

設定	説明
システム名	この vCloud Director インストールに作成する vCenter Server フォルダの名前。デフォルトでは vcd1 です。
インストール ID	仮想 NIC の MAC アドレスを作成するときに使用するこの vCloud Director インストールの ID。デフォルトでは 1 です。  マルチサイト展開の vCloud Director インストール間で拡張ネットワークを作成する予定がある場合は、各 vCloud Director インストールに一意のインストール ID を設定することを検討してください。

- 3 (オプション) ネットワーク トポロジで必要な場合は、[追加のネットワーク プロパティ] セクションに eth0 および eth1 ネットワーク インターフェイスのスタティック ルートを入力し、[次へ] をクリックします。

デフォルト以外のゲートウェイ ルートを經由してホストにアクセスする場合は、スタティック ルートの指定が必要になる場合があります。たとえば、管理インフラストラクチャにアクセスするには、eth1 インターフェイスを使用する必要がありますが、デフォルト ゲートウェイは eth0 に設定されています。通常は、この設定を空のままに構いません。

スタティック ルートは、カンマ区切りリストの形式でルートを指定する必要があります。ルート指定には、ターゲット ゲートウェイの IP アドレスと、オプションとして Classless Inter-Domain Routing (CIDR) ネットワーク指定を含める必要があります。たとえば、**172.16.100.253 172.16.100.0/19, 172.16.200.253** のように指定します。

- 4 [ネットワーク プロパティ] セクションに eth0 NIC および eth1 NIC のネットワークの詳細を入力し、[次へ] をクリックします。

設定	説明
デフォルト ゲートウェイ	アプライアンスのデフォルト ゲートウェイの IP アドレス。
ドメイン名	DNS 検索ドメイン (mydomain.com など)。
ドメイン検索パス	アプライアンスのホスト名検索用のドメイン名のカンマ区切りリストまたはスペース区切りリスト (subdomain.example.com など)。  <b>注：</b> [ドメイン名] テキスト ボックスに入力したドメイン名が、ドメイン検索パス リストの最初の要素になります。
ドメイン ネーム サーバ	アプライアンスのドメイン ネーム サーバの IP アドレス。
eth0 ネットワークの IP アドレス	eth0 インターフェイスの IP アドレス。
eth0 ネットワーク マスク	eth0 インターフェイスのネットマスクまたはプリフィックス。
eth1 ネットワークの IP アドレス	eth1 インターフェイスの IP アドレス。
eth1 ネットワーク マスク	eth1 インターフェイスのネットマスクまたはプリフィックス。

- 5 [設定内容の確認] 画面で、vCloud Director アプライアンスの設定を確認し、[完了] をクリックしてデプロイを開始します。

#### 次のステップ

- 新しく作成した仮想マシンパワーオンします。
- [vCloud Director アプライアンスのタイムゾーンの変更](#)

## VMware OVF Tool を使用した vCloud Director アプライアンスのデプロイ

VMware OVF Tool を使用して、vCloud Director アプライアンスを OVF テンプレートとしてデプロイできます。

vCloud Director サーバ グループの最初のメンバーはプライマリ セルとしてデプロイする必要があります。  
vCloud Director サーバ グループの後続のメンバーは、スタンバイ セルまたは vCD アプリケーション セルとしてデプロイできます。[アプライアンス環境とデータベースの高可用性構成](#)を参照してください。

OVF Tool のインストールの詳細については、『VMware OVF Tool リリース ノート』を参照してください。

OVF Tool の使用方法の詳細については、『OVF Tool ユーザー ガイド』を参照してください。

**重要：** Linux 上の vCloud Director インストールおよび vCloud Director アプライアンス環境を 1 つのサーバ グループ内で混在させることはできません。

追加または置き換えのアプライアンスをデータベース クラスタに追加する場合、vCPU および RAM はクラスタ内の既存のプライマリ セルとスタンバイ セルのものと一致させる必要があります。

新しくデプロイされたスタンバイの OVA のバージョンは、クラスタ内の既存のアプライアンスと同じである必要があります。実行中のアプライアンスのバージョンを確認するには、アプライアンス管理ユーザー インターフェイスのバージョン情報を表示します。アプライアンスは、VMware Cloud Director-v.v.v.-nnnnnn\_OVF10.ova という形式の名前で配布されます。ここで vv.v.v は、製品バージョン、nnnnnn はビルド番号を表します。例：  
VMware Cloud Director-10.2.0.0-9229800\_OVA10.ova

vSphere に OVF テンプレートをデプロイする方法の詳細については、「vSphere 仮想マシン管理」を参照してください。

または、vSphere Client を使用してアプライアンスをデプロイすることもできます。[vSphere Client を使用した vCloud Director アプライアンスのデプロイ](#)を参照してください。

**注：** vCloud Director への vCloud Director アプライアンスのデプロイはサポートされていません。

デプロイ コマンドを実行する前に、[vCloud Director アプライアンスのデプロイの前提条件](#)を参照してください。

アプライアンスをデプロイしたら、firstboot ログ ファイルで警告エラー メッセージを確認します。[vCloud Director アプライアンスのログ ファイルの調査](#)を参照してください。

## vCloud Director アプライアンスをデプロイするための ovftool コマンドのオプションとプロパティ

オプション	値	説明
--noSSLVerify	該当なし	vSphere 接続の SSL 検証をスキップします。
--acceptAllEulas	該当なし	すべてのエンド ユーザー使用許諾契約書 (EULA) を承諾します。
--datastore	target_vc_datastore	仮想マシンの構成ファイルおよび仮想ディスクを格納するターゲット データストアの名前。

オプション	値	説明
--allowAllExtraConfig	該当なし	すべての追加設定オプションを VMX 形式に変換します。
--net:"eth0 Network"	<i>portgroup_on_vc_for_eth0</i>	アプライアンス eth0 ネットワークのターゲット ネットワーク。  <b>重要:</b> eth1 ターゲット ネットワークと異なる ネットワークを指定する必要があります。
--net:"eth1 Network"	<i>portgroup_on_vc_for_eth1</i>	アプライアンス eth1 ネットワークのターゲット ネットワーク。  <b>重要:</b> eth0 ターゲット ネットワークと異なる ネットワークを指定する必要があります。
--name	<i>vm_name_on_vc</i>	アプライアンスの仮想マシン名。
--diskMode	thin または thick	仮想マシンの構成ファイルおよび仮想ディスクのディスク フォーマット。
--prop:"vami.ip0.VMware_vCloud_Director" <i>eth0_ip_address</i>		eth0 の IP アドレス。ユーザー インターフェイスおよび API へのアクセスに使用されます。このアドレスでは、DNS 逆引きによってアプライアンスのホスト名が決定および設定されます。
--prop:"vami.ip1.VMware_vCloud_Director" <i>eth1_ip_address</i>		eth1 の IP アドレス。組み込みの PostgreSQL データベース サービスを含む内部サービスにアクセスする場合に使用されます。
--prop:"vami.DNS.VMware_vCloud_Director" <i>dns_ip_address</i>		アプライアンスのドメイン ネーム サーバの IP アドレス。
--prop:"vami.domain.VMware_vCloud_Director" <i>domain_name</i>		DNS 検索ドメイン。検索パスの最初の要素として表示されます。
--prop:"vami.gateway.VMware_vCloud_Director" <i>gateway_ip_address</i>		アプライアンスのデフォルト ゲートウェイの IP アドレス。
--prop:"vami.netmask0.VMware_vCloud_Director" <i>netmask</i>		eth0 インターフェイスのネットマスクまたはブリフィックス。
--prop:"vami.netmask1.VMware_vCloud_Director" <i>netmask</i>		eth1 インターフェイスのネットマスクまたはブリフィックス。
--prop:"vami.searchpath.VMware_vCloud_Director" <i>searchpath</i>		アプライアンスのドメイン検索パス。ドメイン名のカンマ区切りリストまたはスペース区切りリスト。
--prop:"vcloudapp.enable_ssh.VMware_vCloud_Director" <i>enable_ssh</i>		アプライアンスの root への SSH アクセスを有効または無効にします。
--prop:"vcloudapp.expire_root_password.VMware_vCloud_Director" <i>expire_root_password</i>		最初のログイン後も初期パスワードを使用し続けるかどうかを決定します。
--prop:"vcloudapp.nfs_mount.VMware_vCloud_Director" <i>nfs_ip_address:nfs_mount_path</i>		外部 NFS サーバの IP アドレスとエクスポート パス。  プライマリ セルにのみ使用されます。
--prop:"vcloudapp.ntp-server.VMware_vCloud_Director" <i>ntp_server_ip_address</i>		タイム サーバの IP アドレス。

オプション	値	説明
--prop:"vcloudapp.varoot-password.VMware_vCloud_Director_password"	<del>VMware_vCloud_Director_password</del>	アプライアンスの初期 root パスワード。8 文字以上（大文字、小文字、数字、特殊文字をそれぞれ 1 文字以上）を含める必要があります。  <b>重要：</b> 初期の root パスワードがキーストアのパスワードになります。クラスタ環境では、初期導入時にすべてのセルに同じ root パスワードを設定する必要があります。起動プロセスが完了したら、目的の任意のセルの root パスワードを変更できます。
--prop:"vcloudconf.db_pwd.VMware_vCloud_Director_password"	<del>VMware_vCloud_Director_password</del>	vcloud ユーザーのデータベース パスワード。プライマリ セルにのみ使用されます。
--prop:"vcloudwiz.admin_email.VMware_vCloud_Director_email_address"	<del>VMware_vCloud_Director_email_address</del>	システム管理者アカウントのメール アドレス。プライマリ セルにのみ使用されます。
--prop:"vcloudwiz.admin_fname.VMware_vCloud_Director_admin_fname"	<del>VMware_vCloud_Director_admin_fname</del>	システム管理者アカウントの名前。プライマリ セルにのみ使用されます。
--prop:"vcloudwiz.admin_pwd.VMware_vCloud_Director_admin_password"	<del>VMware_vCloud_Director_admin_password</del>	システム管理者アカウントのパスワード。プライマリ セルにのみ使用されます。
--prop:"vcloudwiz.admin_uname.VMware_vCloud_Director_admin_username"	<del>VMware_vCloud_Director_admin_username</del>	システム管理者アカウントのユーザー名。プライマリ セルにのみ使用されます。
--prop:"vcloudwiz.inst_id.VMware_vCloud_Director_inst_ID"	<del>VMware_vCloud_Director_inst_ID</del>	vCloud Director インストール ID。プライマリ セルにのみ使用されます。
--prop:"vcloudconf.sys_name.VMware_vCloud_Director_system_name"	<del>VMware_vCloud_Director_system_name</del>	この vCloud Director インストールに作成する vCenter Server フォルダの名前。
--prop:"vcloudnet.routes0.VMware_vCloud_Director_routes0_cidr, ip_address2, ..."	<del>VMware_vCloud_Director_routes0_cidr, ip_address2, ...</del>	オプション。eth0 インターフェイスのステイック ルート。カンマ区切りリストの形式でルートを指定する必要があります。ルート指定には、ゲートウェイ IP アドレスと、オプションで Classless Inter-Domain Routing (CIDR) ネットワーク指定（プリフィックス/ビット）を含める必要があります。たとえば、 <b>172.16.100.253 172.16.100/19, 172.16.200.253</b> のようになります。
--prop:"vcloudnet.routes1.VMware_vCloud_Director_routes1_cidr, ip_address2, ..."	<del>VMware_vCloud_Director_routes1_cidr, ip_address2, ...</del>	オプション。eth1 インターフェイスのステイック ルート。カンマ区切りリストの形式でルートを指定する必要があります。ルート指定には、ゲートウェイ IP アドレスと、オプションで Classless Inter-Domain Routing (CIDR) ネットワーク指定（プリフィックス/ビット）を含める必要があります。たとえば、 <b>172.16.100.253 172.16.100/19, 172.16.200.253</b> のように指定します。

オプション	値	説明
--deploymentOption	primary-small、primary-large、standby-small、standby-large、または cell	<p>デプロイするアプライアンスのタイプとサイズ。プライマリ（小）およびスタンバイ（小）アプライアンス サイズは、ラボ システムまたはテストシステムに適しています。プライマリ（大）およびスタンバイ（大）のサイズは、本番環境システムの最小のサイズ要件を満たします。ワークロードによっては、リソースの追加が必要になる場合があります。</p> <ul style="list-style-type: none"> <li>■ primary-small は 12 GB の RAM と 2 つの vCPU を搭載したアプライアンスを、vCloud Director サーバ グループの最初のメンバーとしてデプロイします。プライマリ セルの組み込みデータベースは、vCloud Director データベースとして設定されます。データベース名は vcloud、データベース ユーザーは vcloud です。</li> <li>■ primary-large は 24 GB の RAM と 4 つの vCPU を搭載したアプライアンスを、vCloud Director サーバ グループの最初のメンバーとしてデプロイします。プライマリ セルの組み込みデータベースは、vCloud Director データベースとして設定されます。データベース名は vcloud、データベース ユーザーは vcloud です。</li> <li>■ standby-small は 12 GB の RAM と 2 つの vCPU を搭載したアプライアンスを、データベース高可用性構成の vCloud Director サーバ グループの 2 番目または 3 番目のメンバーとしてデプロイします。スタンバイ セルの組み込みデータベースは、プライマリ データベースを使用してレプリケーション モードで設定されます。</li> <li>■ standby-large は 24 GB の RAM と 4 つの vCPU を搭載したアプライアンスを、データベース高可用性構成の vCloud Director サーバ グループの 2 番目または 3 番目のメンバーとしてデプロイします。スタンバイ セルの組み込みデータベースは、プライマリ データベースを使用してレプリケーション モードで設定されます。</li> <li>■ cell は 8 GB の RAM と 2 つの vCPU を搭載したアプライアンスを、vCloud Director サーバ グループの後続のメンバーとしてデプロイします。vCD アプリケ</li> </ul>

オプション	値	説明
		<p>ーション セル内の組み込みデータベースは使用されません。vCD アプリケーションセルは、プライマリ データベースに接続されます。</p> <p><b>重要：</b> vCloud Director サーバ グループ内のプライマリ セルおよびスタンバイ セルは、同じサイズである必要があります。データベース HA クラスターは、1つのプライマリ セル（小）と 2つのスタンバイ セル（小）、または1つのプライマリ セル（大）と 2つのスタンバイ セル（大）で構成できます。</p> <p>デプロイ後に、アプライアンスのサイズを再構成できます。</p>
--powerOn	<i>path_to_ova</i>	デプロイ後、仮想マシンをパワーオンします。

## プライマリ vCloud Director アプライアンスをデプロイするコマンドの例

**重要：** VMware OVF Tool コマンドを実行する前に、vcloudapp.varoot-passwordVMware\_vCloud\_Director、vcloudconf.db\_pwdVMware\_vCloud\_Director、およびvcloudconf.admin\_pwd.VMware\_vCloud\_Director パスワード を独自の安全なパスワードと置き換えます。

```
ovftool \
--noSSLVerify \
--acceptAllEulas \
--datastore='datastore6' \
--allowAllExtraConfig \
--net:"eth0 Network"="My_UI_API_Network" \
--net:"eth1 Network"="My_Internal_DB_Services_Network" \
--name=MyAppliance \
--diskMode=thin \
--prop:"vami.ip0.VMware_vCloud_Director"="10.0.0.142" \
--prop:"vami.ip1.VMware_vCloud_Director"="172.18.41.24" \
--prop:"vami.DNS.VMware_vCloud_Director"="10.0.0.2" \
--prop:"vami.domain.VMware_vCloud_Director"="mycompany.com" \
--prop:"vami.gateway.VMware_vCloud_Director"="10.0.0.1" \
--prop:"vami.netmask0.VMware_vCloud_Director"="255.255.0.0" \
--prop:"vami.netmask1.VMware_vCloud_Director"="255.255.224.0" \
--prop:"vami.searchpath.VMware_vCloud_Director"="eng.mycompany.com" \
--prop:"vcloudapp.enable_ssh.VMware_vCloud_Director"="False" \
--prop:"vcloudapp.expire_root_password.VMware_vCloud_Director"="True" \
--prop:"vcloudapp.nfs_mount.VMware_vCloud_Director"="10.0.0.96:/data/transfer" \
--prop:"vcloudapp.ntp_server.VMware_vCloud_Director"="time.mycompany.com" \
--prop:"vcloudapp.varoot_password.VMware_vCloud_Director"="place-secure-password-here" \
--prop:"vcloudconf.db_pwd.VMware_vCloud_Director"="place-secure-password-here" \
--prop:"vcloudconf.admin_email.VMware_vCloud_Director"="admin@mycompany.com" \
--prop:"vcloudconf.admin_fname.VMware_vCloud_Director"="vcdadmin" \
--prop:"vcloudconf.admin_pwd.VMware_vCloud_Director"="place-secure-password-here" \
--prop:"vcloudconf.admin_uname.VMware_vCloud_Director"="administrator" \
--prop:"vcloudconf.inst_id.VMware_vCloud_Director"="59" \
```

```
--prop:"vcloudconf.sys_name.VMware_vCloud_Director"="MyAppliance" \
--deploymentOption="primary-small" \
--powerOn "/MyPath/VMware_vCloud_Director-version_number_OVF10.ova" \
vi://vc_user_name:vc_password@vc_hostname_or_ip_address/vc_datacenter_name/host/vc_cluster_name
```

## スタンバイ vCloud Director アプライアンスをデプロイするコマンドの例

**重要：** VMware OVF Tool コマンドを実行する前に、vcloudapp.varoot-password.VMware\_vCloud\_Director パスワードを独自の安全なパスワードと置き換えます。

```
ovftool \
--noSSLVerify \
--acceptAllEulas \
--datastore='datastore6' \
--allowAllExtraConfig \
--net:"eth0 Network"="My_UI_API_Network" \
--net:"eth1 Network"="My_Internal_DB_Services_Network" \
--name=MySecondAppliance \
--diskMode=thin \
--prop:"vami.ip0.VMware_vCloud_Director"="10.0.0.143" \
--prop:"vami.ip1.VMware_vCloud_Director"="172.18.41.25" \
--prop:"vami.DNS.VMware_vCloud_Director"="10.0.0.2" \
--prop:"vami.domain.VMware_vCloud_Director"="mycompany.com" \
--prop:"vami.gateway.VMware_vCloud_Director"="10.0.0.1" \
--prop:"vami.netmask0.VMware_vCloud_Director"="255.255.0.0" \
--prop:"vami.netmask1.VMware_vCloud_Director"="255.255.224.0" \
--prop:"vami.searchpath.VMware_vCloud_Director"="eng.mycompany.com" \
--prop:"vcloudapp.enable_ssh.VMware_vCloud_Director"="False" \
--prop:"vcloudapp.expire_root_password.VMware_vCloud_Director"="True" \
--prop:"vcloudapp.nfs_mount.VMware_vCloud_Director"="10.0.0.96:/data/transfer" \
--prop:"vcloudapp.ntp-server.VMware_vCloud_Director"="time.mycompany.com" \
--prop:"vcloudapp.varoot-password.VMware_vCloud_Director"="place-secure-password-here" \
--prop:"vcloudconf.sys_name.VMware_vCloud_Director"="MySecondAppliance" \
--deploymentOption="standby-small" \
--powerOn "/MyPath/VMware_vCloud_Director-version_number_OVF10.ova" \
vi://vc_user_name:vc_password@vc_hostname_or_ip_address/vc_datacenter_name/host/vc_cluster_name
```



# vCloud Director アプライアンス SSL 証明書

# 7

vCloud Director アプライアンスでは、クライアントとサーバ間で安全な通信を行うために SSL を使用します。各 vCloud Director アプライアンスは、HTTPS 用とコンソール プロキシ通信用の 2 台の異なる SSL エンドポイントをサポートしている必要があります。

これらのエンドポイントには異なる IP アドレスを割り当てることもできますし、同じ IP アドレスで 2 つの異なるポートを割り当てることもできます。各エンドポイントには独自の SSL 証明書が必要です。両方のエンドポイントに同じ証明書（ワイルドカード証明書など）を使用できます。

この章には、次のトピックが含まれています。

- [HTTPS 通信およびコンソール プロキシ通信用の署名付きワイルドカード証明書を使用した vCloud Director アプライアンスのデプロイ](#)
- [vCloud Director アプライアンスへの CA 署名付き SSL 証明書の作成とインポート](#)
- [プライベート キーおよび CA 署名付き SSL 証明書の vCloud Director アプライアンスへのインポート](#)
- [自己署名の組み込み PostgreSQL および vCloud Director アプライアンスの管理ユーザー インターフェイス証明書の置き換え](#)
- [vCloud Director アプライアンス証明書の更新](#)

## HTTPS 通信およびコンソール プロキシ通信用の署名付きワイルドカード証明書を使用した vCloud Director アプライアンスのデプロイ

署名付きワイルドカード証明書を使用して、vCloud Director アプライアンスをデプロイできます。これらの証明書を使用すると、証明書にリストされているドメイン名のサブドメインであるサーバを、数に制限なく保護できます。

デフォルトでは、vCloud Director アプライアンスをデプロイすると、vCloud Director は自己署名証明書を生成し、それらを使用して HTTPS 通信およびコンソール プロキシ通信用の vCloud Director セルを設定します。

プライマリ アプライアンスを正常にデプロイすると、アプライアンス構成ロジックによって、プライマリ アプライアンスから共通の NFS 共有転送サービス ストレージ (/opt/vmware/vcloud-director/data/transfer) に responses.properties ファイルがコピーされます。この vCloud Director サーバ グループにデプロイされた他のアプライアンスは、このファイルを使用して自動的に設定されます。responses.properties ファイルには SSL 証明書キーストアのパスが含まれていて、SSL 証明書キーストアには自動生成された自己署名証明書 user.keystore.path が含まれています。デフォルトでは、このパスは各アプライアンスに対してローカルなキーストア ファイルのパスになります。

プライマリ アプライアンスをデプロイした後で、署名付き証明書を使用するように再設定できます。署名付き証明書を使用したキーストアの作成の詳細については、[vCloud Director アプライアンスへの CA 署名付き SSL 証明書の作成とインポート](#)を参照してください。

プライマリ vCloud Director アプライアンスで使用する署名付き証明書が署名付きワイルドカード証明書である場合、これらの証明書は vCloud Director サーバ グループ内の他のすべてのアプライアンス、つまりスタンバイ セルと vCloud Director アプリケーション セルに適用できます。HTTPS 通信およびコンソール プロキシ通信の署名付きワイルドカード証明書を使用したアプライアンスのデプロイを行って、追加のセルに署名付きワイルドカード SSL 証明書を設定できます。

#### 前提条件

- HTTPS とコンソール プロキシの両方のエイリアス用の署名付きワイルドカード SSL 証明書を含むキーストアが、プライマリ アプライアンス (/opt/vmware/vcloud-director/certificates.ks) で使用可能であることを確認します。
  - キーペアを作成し、CA 署名付き証明書ファイルをインポートする必要がある場合は、[vCloud Director アプライアンスへの CA 署名付き SSL 証明書の作成とインポート](#)を参照してください。
  - 独自のプライベート キー ファイルと CA 署名付き証明書ファイルがすでに存在する場合は、[プライベート キーおよび CA 署名付き SSL 証明書の vCloud Director アプライアンスへのインポート](#)を参照してください。
- キーストア内のキーのプライベート パスワードがキーストアのパスワードと一致することを確認します。キーストアのパスワードは、次のような、すべてのアプライアンスをデプロイするときに使用する初期 root パスワードと一致する必要があります。

```
/opt/vmware/vcloud-director/jre/bin/keytool -keypasswd -alias http_or_consoleproxy -keystore /opt/vmware/vcloud-director/certificates.ks -storetype jceks -storepass root-password
```

。

#### 手順

- 1 プライマリ アプライアンスから転送共有 (/opt/vmware/vcloud-director/data/transfer/) に、適切に署名された証明書を含む新しい certificates.ks ファイルをコピーします。
- 2 キーストア ファイルに関する所有者およびグループの権限を **vcld** に変更します。

```
chown vcld.vcld /opt/vmware/vcloud-director/data/transfer/certificates.ks
```

- 3 キーストア ファイルの所有者に読み取りおよび書き込み権限があることを確認します。

```
chmod 0750 /opt/vmware/vcloud-director/data/transfer/certificates.ks
```

- 4 プライマリ アプライアンスでコマンドを実行して、新しい署名付き証明書を vCloud Director インスタンスにインポートします。

このコマンドにより、転送共有内の `responses.properties` ファイルも更新され、転送共有内のキーストア ファイルを参照するように `user.keystore.path` 変数が変更されます。

```
/opt/vmware/vcloud-director/bin/cell-management-tool certificates -j -p --keystore /opt/vmware/vcloud-director/data/transfer/certificates.ks --keystore-password root-password
```

- 5 新しい署名付き証明書を有効にするには、プライマリ アプライアンスで `vmware-vcd` サービスを再起動します。

```
service vmware-vcd restart
```

- 6 キーストアのパスワードと一致する初期 root パスワードを使用して、スタンバイ セル アプライアンスとアプリケーション セル アプライアンスをデプロイします。

## 結果

新しくデプロイされたアプライアンスのうち、同じ NFS 共有転送サービス ストレージを使用するものはすべて、プライマリ アプライアンスで使用されるものと同じ署名付きワイルドカード SSL 証明書を使用して設定されます。

## vCloud Director アプライアンスへの CA 署名付き SSL 証明書の作成とインポート

認証局 (CA) によって署名された証明書を作成およびインポートすると、SSL 通信の信頼レベルが最大になり、クラウド内の接続を保護することができます。

各 vCloud Director サーバには、クライアントとサーバ間の通信を保護するために 2 つの SSL 証明書が必要です。各 vCloud Director サーバは、HTTPS 用とコンソール プロキシ通信用の 2 つの異なる SSL エンドポイントをサポートしている必要があります。

vCloud Director アプライアンスでは、これら 2 台のエンドポイントは同じ IP アドレスまたはホスト名を共有しますが、2 つの個別のポート (HTTPS には 443、コンソール プロキシ通信には 8443) を使用します。各エンドポイントには独自の SSL 証明書が必要です。ワイルドカード証明書を使用するなど、両方のエンドポイントに同じ証明書を使用できます。

いずれのエンドポイントの証明書にも、X.500 識別名と X.509 サブジェクトの別名拡張機能が含まれている必要があります。

独自のプライベート キー ファイルと CA 署名付き証明書ファイルがすでに存在する場合は、[プライベート キーおよび CA 署名付き SSL 証明書の vCloud Director アプライアンスへのインポート](#)に記載されている手順を実行します。

**重要：** デプロイ時に、vCloud Director アプライアンスは、2,048 ビットのキー サイズの自己署名証明書を生成します。適切なキー サイズを選択する前に、インストールのセキュリティ要件を評価する必要があります。NIST Special Publication 800-131A に従い、1024 ビット未満のキー サイズはサポートされなくなりました。

この手順で使用されるキーストア パスワードは root ユーザー パスワードであり、`root_passwd` として表されます。

#### 前提条件

`keytool` コマンドについて理解しておきます。`keytool` を使用して、CA 署名付き SSL 証明書を vCloud Director アプライアンスにインポートします。vCloud Director は、`keytool` のコピーを `/opt/vmware/vcloud-director/jre/bin/keytool` に配置します。

#### 手順

- 1 vCloud Director アプライアンス コンソールに root として直接ログインするか、SSH で接続します。
- 2 環境のニーズに応じて、次のいずれかのオプションを選択します。

vCloud Director アプライアンスをデプロイすると、vCloud Director は、HTTPS サービスとコンソール プロキシ サービス用に 2,048 ビットのキー サイズで自己署名証明書を自動的に生成します。

- デプロイ時に生成される証明書に認証局で署名する場合は、[手順 手順 5](#) に進みます。
- キー サイズを大きくするなどのカスタム オプションを使用して新しい証明書を生成する場合は、[手順 手順 3](#) に進みます。

- 3 コマンドを実行して、既存の `certificates.ks` ファイルをバックアップします。

```
cp /opt/vmware/vcloud-director/certificates.ks /root/certificates.ks.original
```

- 4 コマンドを実行して、HTTPS サービス用とコンソール プロキシ サービス用のパブリックおよびプライベート キー ペアを作成します。

```
/opt/vmware/vcloud-director/bin/cell-management-tool generate-certs -j -p -o /opt/vmware/vcloud-director/certificates.ks -w root_passwd
```

このコマンドにより、指定したパスワードを使用して、`certificates.ks` でキーストアが作成または更新されます。証明書はコマンドのデフォルト値を使用して作成されます。環境の DNS 構成に応じて、発行者のコモン ネーム (CN) は各サービスの IP アドレスまたは FQDN に設定されます。証明書はキー長にデフォルトの 2048 ビットを使用し、作成後 1 年で期限切れになります。

---

**重要：** vCloud Director アプライアンスの構成上の制限により、証明書キーストアに場所 `/opt/vmware/vcloud-director/certificates.ks` を使用する必要があります。

---



---

**注：** アプライアンスの root パスワードをキーストア パスワードとして使用します。

---

## 5 HTTPS サービス用とコンソール プロキシ サービス用の証明書署名リクエスト (CSR) を作成します。

**重要：** vCloud Director アプライアンスは、HTTPS サービスとコンソール プロキシ サービスの両方で同じ IP アドレスおよびホスト名を共有します。そのため、CSR 作成コマンドでは、Subject Alternative Names (SAN) 拡張引数に同じ DNS および IP アドレスを指定する必要があります。

- a `http.csr` ファイル内に証明書署名リクエストを作成します。

```
keytool -keystore certificates.ks -storetype JCEKS -storepass root_password -certreq -alias http -file http.csr -ext "san=dns:vcd2.example.com,dns:vcd2,ip:10.100.101.10"
```

- b `consoleproxy.csr` ファイル内に証明書署名リクエストを作成します。

```
keytool -keystore certificates.ks -storetype JCEKS -storepass root_password -certreq -alias consoleproxy -file consoleproxy.csr -ext "san=dns:vcd2.example.com,dns:vcd2,ip:10.100.101.10"
```

## 6 証明書署名リクエストを認証局に送信します。

証明書発行機関により、Web サーバー タイプを指定するよう求められる場合は、Jakarta Tomcat を使用します。

CA 署名付き証明書を取得します。

## 7 CA 署名付き証明書、CA ルート証明書、および任意の中間証明書を vCloud Director アプライアンスにコピーします。

## 8 コマンドを実行して、署名付き証明書を JCEKS キーストアにインポートします。

- a `root.cer` ファイルから `certificates.ks` キーストア ファイルに認証局のルート証明書をインポートします。

```
keytool -import -storetype JCEKS -storepass root_password -keystore /opt/vmware/vcloud-director/certificates.ks -alias root -file root_certificate_file
```

- b 中間証明書を受信した場合は、この証明書を `intermediate.cer` ファイルから `certificates.ks` キーストア ファイルにインポートします。

```
keytool -import -storetype JCEKS -storepass root_password -keystore /opt/vmware/vcloud-director/certificates.ks -alias intermediate -file intermediate_certificate_file
```

- c HTTPS サービス証明書をインポートします。

```
keytool -import -storetype JCEKS -storepass root_password -keystore /opt/vmware/vcloud-director/certificates.ks -alias http -file http_certificate_file
```

- d コンソール プロキシ サービスの証明書をインポートします。

```
keytool -import -storetype JCEKS -storepass root_password -keystore /opt/vmware/vcloud-director/certificates.ks -alias consoleproxy -file console_proxy_certificate_file
```

これらのコマンドは、`certificates.ks` ファイルを新しく取得した CA 署名付きバージョンの証明書で上書きします。

- 9 証明書がインポートされているかどうかを確認するには、次のコマンドを実行してキーストア ファイルの内容を一覧表示します。

```
keytool -storetype JCEKS -storepass root_password -keystore /opt/vmware/vcloud-director/
certificates.ks -list
```

- 10 コマンドを実行して、証明書を vCloud Director インスタンスにインポートします。

```
/opt/vmware/vcloud-director/bin/cell-management-tool certificates -j -p --keystore /opt/vmware/
vcloud-director/certificates.ks --keystore-password root_password
```

- 11 新しい署名付き証明書を有効にするには、vCloud Director アプライアンスで vmware-vcd サービスを再起動します。

```
service vmware-vcd restart
```

#### 次のステップ

- ワイルドカード証明書を使用する場合は、[HTTPS 通信およびコンソール プロキシ通信用の署名付きワイルドカード証明書を使用した vCloud Director アプライアンスのデプロイ](#)を参照してください。
- ワイルドカード証明書を使用しない場合は、サーバ グループ内のすべての vCloud Director サーバでこの手順を繰り返します。
- 組み込みの PostgreSQL データベースおよび vCloud Director アプライアンスの管理ユーザー インターフェイスの証明書の置換の詳細については、[自己署名の組み込み PostgreSQL および vCloud Director アプライアンスの管理ユーザー インターフェイス証明書の置き換え](#)を参照してください。

## プライベート キーおよび CA 署名付き SSL 証明書の vCloud Director アプライアンスへのインポート

独自のプライベート キーおよび CA 署名付き証明書ファイルがある場合は、キーストアを vCloud Director 環境にインポートする前に、HTTPS サービスとコンソール プロキシ サービスの両方の証明書とプライベート キーをインポートするキーストア ファイルを作成する必要があります。

#### 前提条件

- keytool コマンドについて理解しておきます。keytool を使用して、CA 署名付き SSL 証明書を vCloud Director アプライアンスにインポートします。vCloud Director は、keytool のコピーを /opt/vmware/vcloud-director/jre/bin/keytool に配置します。
- 中間証明書、ルート CA 証明書、CA 署名付き HTTPS サービス、およびコンソール プロキシ サービスのプライベート キーと証明書をアプライアンスにコピーします。

#### 手順

- 1 vCloud Director アプライアンス コンソールに root として直接ログインするか、SSH で接続します。

- 2 中間証明書がある場合は、コマンドを実行してルート CA 署名証明書と中間証明書を結合し、証明書チェーンを作成します。

```
cat intermediate-certificate-file-1.cer intermediate-certificate-file-2.cer root-CA-certificate.cer > chain.crt
```

- 3 OpenSSL を使用して、HTTPS サービスとコンソール プロキシ サービスの両方のために、プライベート キー、証明書チェーン、それぞれのエイリアスを持つ中間 PKCS12 キーストア ファイルを作成し、各キーストア ファイルのパスワードを指定します。

- a HTTPS サービス用のキーストア ファイルを作成します。

```
openssl pkcs12 -export -in http.crt -inkey http.key -CAfile chain.crt -name http -passout pass:keystore_password -out http.pfx -chain
```

- b コンソール プロキシ サービス用のキーストア ファイルを作成します。

```
openssl pkcs12 -export -in consoleproxy.crt -inkey consoleproxy.key -CAfile chain.crt -name consoleproxy -passout pass:keystore_password -out consoleproxy.pfx -chain
```

- 4 コマンドを実行して、既存の certificates.ks ファイルをバックアップします。

```
cp /opt/vmware/vcloud-director/certificates.ks /root/certificates.ks.original
```

- 5 keytool コマンドを使用して、PKCS12 キーストアを JCEKS キーストアにインポートします。

- a HTTPS サービス用に PKCS12 キーストアをインポートします。

```
keytool -importkeystore -deststorepass keystore_password -destkeystore /opt/vmware/vcloud-director/certificates.ks -deststoretype JCEKS -srckeystore http.pfx -srcstoretype PKCS12 -srcstorepass keystore_password
```

- b コンソール プロキシ サービス用に PKCS12 キーストアをインポートします。

```
keytool -importkeystore -deststorepass keystore_password -destkeystore /opt/vmware/vcloud-director/certificates.ks -deststoretype JCEKS -srckeystore consoleproxy.pfx -srcstoretype PKCS12 -srcstorepass keystore_password
```

- 6 証明書のインポートが成功したことを確認します。

```
keytool -storetype JCEKS -storepass keystore_password -keystore /opt/vmware/vcloud-director/certificates.ks -list
```

- 7 コマンドを実行して、署名付き証明書を vCloud Director インスタンスにインポートします。

```
/opt/vmware/vcloud-director/bin/cell-management-tool certificates -j -p --keystore /opt/vmware/vcloud-director/certificates.ks --keystore-password keystore_password
```

- 8 CA 署名付き証明書を有効にするには、vCloud Director アプライアンスで vmware-vcd サービスを再起動します。

```
service vmware-vcd restart
```

## 次のステップ

- ワイルドカード証明書を使用する場合は、[HTTPS 通信およびコンソール プロキシ通信用の署名付きワイルドカード証明書を使用した vCloud Director アプライアンスのデプロイ](#)を参照してください。
- ワイルドカード証明書を使用しない場合は、サーバ グループ内のすべての vCloud Director アプライアンスセルでこの手順を繰り返します。
- 組み込みの PostgreSQL データベースおよび vCloud Director アプライアンスの管理ユーザー インターフェイスの証明書の置換の詳細については、[自己署名の組み込み PostgreSQL および vCloud Director アプライアンスの管理ユーザー インターフェイス証明書の置き換え](#)を参照してください。

## 自己署名の組み込み PostgreSQL および vCloud Director アプライアンスの管理ユーザー インターフェイス証明書の置き換え

デフォルトでは、組み込み PostgreSQL データベースおよび vCloud Director アプライアンスの管理ユーザー インターフェイスは、一連の自己署名の SSL 証明書を共有します。セキュリティを強化するために、デフォルトの自己署名証明書を認証局 (CA) が署名した証明書に置き換えることができます。

vCloud Director アプライアンスをデプロイすると、有効期間が 365 日の自己署名証明書が生成されます。vCloud Director アプライアンスは 2 セットの SSL 証明書を使用します。vCloud Director サービスは、HTTPS およびコンソール プロキシの通信に 1 セットの証明書を使用します。組み込み PostgreSQL データベースおよび vCloud Director アプライアンスの管理ユーザー インターフェイスは、別の SSL 証明書セットを共有します。

**注：** データベースおよびアプライアンス管理ユーザー インターフェイスの証明書を置き換えるプロセスは、HTTPS およびコンソール プロキシ通信の証明書には影響しません。証明書セットの一方を置き換えても、他方のセットの置き換えが必要になるわけではありません。

## 手順

- 1 `/opt/vmware/appliance/etc/ssl/vcd_ova.csr` にある証明書署名リクエストを認証局 (CA) に送信して、署名するよう要求します。
- 2 プライマリ データベースの証明書を置き換える場合は、データの損失を招くことがないように、他のすべてのノードをメンテナンス モードにします。
- 3 `/opt/vmware/appliance/etc/ssl/vcd_ova.crt` の既存の PEM 形式証明書を、[手順 1](#) で CA から取得した署名付き証明書に置き換えます。
- 4 新しい証明書を取得するには、`vpostgres`、`nginx`、および `vcd_ova_ui` サービスを再起動します。

```
systemctl restart nginx.service && systemctl restart vcd_ova_ui.service
```

```
systemctl restart vpostgres.service
```

- 5 プライマリ データベースの証明書を置き換える場合は、他のすべてのノードでメンテナンス モードを解除します。



## 結果

新しい証明書は、appliance-sync 機能が次回実行されるときに、他の vCloud Director セル上の vCloud Director トラストストアにインポートされます。この操作には、60 秒ほどかかる場合があります。

## vCloud Director アプライアンス証明書の更新

vCloud Director アプライアンスをデプロイすると、有効期間が 365 日の自己署名証明書が生成されます。使用環境で期限切れ間近の証明書または期限切れになった証明書がある場合は、新しい自己署名証明書を生成できます。各 vCloud Director セルの証明書を個別に更新する必要があります。

vCloud Director アプライアンスは 2 セットの SSL 証明書を使用します。vCloud Director サービスは、HTTPS およびコンソール プロキシの通信に 1 セットの証明書を使用します。組み込み PostgreSQL データベースおよび vCloud Director アプライアンスの管理ユーザー インターフェイスは、別の SSL 証明書セットを共有します。

自己署名証明書セットは両方とも変更できます。また、vCloud Director の HTTPS 通信およびコンソール プロキシ通信に CA 署名付き証明書を使用している場合、組み込みの PostgreSQL データベースおよびアプライアンス管理ユーザー インターフェイス証明書のみを変更することもできます。CA 署名付き証明書には、既知の公開認証局をルートとする完全な信頼チェーンが含まれています。

### 前提条件

データベース高可用性クラスタ内のプライマリ ノードの証明書を更新する場合は、データの損失を防ぐために、他のすべてのノードをメンテナンス モードにします。[セルの管理](#)を参照してください。

### 手順

- 1 vCloud Director アプライアンスの OS に root として直接ログインするか、SSH で接続します。
- 2 vCloud Director サービスを停止するには、次のコマンドを実行します。

```
/opt/vmware/vcloud-director/bin/cell-management-tool -u administrator cell --shutdown
```

- 3 新しい自己署名証明書を生成するには、次のコマンドを実行します。

```
/opt/vmware/appliance/bin/generate-certificates.sh <root-password>
```

このコマンドは、組み込みの PostgreSQL データベースおよびアプライアンス管理ユーザー インターフェイスに新しく生成された証明書が使用されるように自動設定します。PostgreSQL サーバと Nginx サーバが再起動します。このコマンドにより、新しい証明書キーストア `/opt/vmware/vcloud-director/certificates.ks` と、[手順 4](#) で使用される vCloud Director の HTTPS 通信およびコンソール プロキシ通信の新しい自己署名証明書が生成されます。

- 4 CA 署名付き証明書を使用していない場合は、コマンドを実行して、新しく生成された自己署名証明書を vCloud Director にインポートします。

```
/opt/vmware/vcloud-director/bin/cell-management-tool certificates -j -p --keystore /opt/vmware/vcloud-director/certificates.ks --keystore-password <root-password>
```

## 5 vCloud Director サービスを再起動します。

```
service vmware-vcd start
```

### 結果

更新された自己署名証明書が、vCloud Director ユーザー インターフェイスに表示されます。

新しい PostgreSQL 証明書は、次回に `appliance-sync` 機能が実行されるときに、他の vCloud Director セル上の vCloud Director トラストストアにインポートされます。この操作には、60 秒ほどかかる場合があります。

### 次のステップ

必要に応じて、自己署名証明書を、外部または内部の認証局によって署名された証明書に置き換えることができます。

# vCloud Director アプライアンスの構成

# 8

データベース HA クラスタ内のセルのステータスの表示、組み込みのデータベースのバックアップおよびリストア、アプライアンスの設定の再構成が可能です。

vCloud Director アプライアンスをデプロイした後で、アプライアンスの eth0 および eth1 ネットワーク IP アドレスやホスト名を変更することはできません。vCloud Director アプライアンスに別のアドレスまたはホスト名を設定するには、新しいアプライアンスをデプロイする必要があります。

アプライアンスのメンテナンスを実行してデータベース高可用性クラスタをシャットダウンする必要がある場合は、同期の問題を回避するために、プライマリ アプライアンスを先にシャットダウンしてからスタンバイ アプライアンスをシャットダウンする必要があります。

この章には、次のトピックが含まれています。

- [データベースの高可用性クラスタ内のセルのステータスの表示](#)
- [高可用性クラスタのプライマリ データベース障害からのリカバリ](#)
- [高可用性クラスタのスタンバイ セル障害からのリカバリ](#)
- [vCloud Director アプライアンスの組み込みデータベースのバックアップとリストア](#)
- [vCloud Director データベースへの外部アクセスの設定](#)
- [vCloud Director アプライアンスへの SSH アクセスの有効化または無効化](#)
- [vCloud Director アプライアンスの DNS 設定の編集](#)
- [vCloud Director アプライアンス ネットワーク インターフェイスのスタティック ルートの編集](#)
- [vCloud Director アプライアンスの構成スクリプト](#)
- [vCloud Director アプライアンスの組み込み PostgreSQL データベースの容量の増加](#)
- [vCloud Director アプライアンスでの PostgreSQL 設定の変更](#)

## データベースの高可用性クラスタ内のセルのステータスの表示

アプライアンス データベース高可用性 (HA) クラスタ内のプライマリ セルおよびスタンバイ セルのステータスを表示するには、データベース HA クラスタの任意のセルのアプライアンス管理ユーザー インターフェイスにログインします。

vCloud Director アプライアンス データベース HA クラスタは、1 つのプライマリ セルと 2 つのスタンバイ セルで構成されます。[アプライアンス環境とデータベースの高可用性構成](#)を参照してください。

## 手順

- 1 Web ブラウザで、[https://vcd\\_ip\\_address:5480](https://vcd_ip_address:5480) のアプライアンス管理ユーザー インターフェイスに移動します。
- 2 root としてログインします。
- 3 データベース HA クラスタ内のセルに関する詳細を表示するには、[vCD データベースの可用性] をクリックします。

プロパティ	説明
名前	セルの DNS 名。
ロール	プライマリまたはスタンバイのいずれかです。 アプライアンス データベース HA クラスタは、1 つのプライマリ セルと 2 つのスタンバイ セルで構成されます。
ステータス	実行中、到達不可、または失敗のいずれかです。 アスタリスク (*) は、プライマリ セルのステータスを示します。
レプリケート元	スタンバイ セルがレプリケートするプライマリ セルの名前。

## 次のステップ

スタンバイ セルが実行状態でない場合は、新しいスタンバイ セルをデプロイします。

プライマリ セルが実行状態でない場合は、[高可用性クラスタのプライマリ データベース障害からのリカバリ](#)を参照してください。

## 高可用性クラスタのプライマリ データベース障害からのリカバリ

プライマリ セルが適切に実行されていない場合に、vCloud Director データベースをリカバリするには、いずれかのスタンバイ セルを昇格させて新しいプライマリ セルにします。その後、新しいスタンバイ セルをデプロイする必要があります。

このワークフローを使用することで、新しいスタンバイをデプロイするときに、障害が発生したプライマリの IP アドレスとホスト名を再利用できます。

## 前提条件

- プライマリ セルがアクセス不可または失敗状態になっていることを確認します。
- 2 つのスタンバイ セルが実行状態になっていることを確認します。
- 障害が発生したアプライアンスを vCloud Director サーバ グループおよび repmgr 高可用性クラスタから削除する手順について理解しておきます。[データベース高可用性クラスタ内の障害の発生したプライマリ セルの登録解除](#)を参照してください。

[データベースの高可用性クラスタ内のセルのステータスの表示](#)を参照してください。

## 手順

- 1 可能であれば、セル管理ツールを使用して vCloud Director プロセスをシャットダウンします。障害が発生したプライマリ セルから次のコマンドを実行します。

```
/opt/vmware/vcloud-director/bin/cell-management-tool -u <admin username> cell --shutdown
```

- 2 障害が発生したプライマリ仮想マシンをパワーオフします。
- 3 実行中のスタンバイ セルのアプライアンス管理ユーザー インターフェイスに root としてログインします ([https://standby\\_ip\\_address:5480](https://standby_ip_address:5480))。
- 4 新しいプライマリ セルにするスタンバイ セルの [ロール] 列で、[昇格] をクリックします。  
このセルが実行状態の新しいプライマリ セルになります。その他のスタンバイ セルは、新しく昇格されたプライマリ セルに従います。
- 5 障害が発生したプライマリ アプライアンスを、vCloud Director サーバ グループと repmgr 高可用性クラスタの両方から削除します。
- 6 障害のあるプライマリの IP アドレスとホスト名を再利用する場合は、障害のあるプライマリ アプライアンスをパワーオフ状態のままにするか、削除します。
- 7 新しいスタンバイ アプライアンスをデプロイします。 [vCloud Director アプライアンスのデプロイの開始](#) ことも、 [VMware OVF Tool を使用した vCloud Director アプライアンスのデプロイ](#) こともできます。

新しいスタンバイ アプライアンスをデプロイした後に、クラスタの健全性は **健全** になっている必要があります。

## 高可用性クラスタのスタンバイ セル障害からのリカバリ

スタンバイ セルが適切に実行されていない場合、障害からリカバリするには、新規スタンバイ セルをデプロイします。

いずれかのスタンバイ セルの状態が Unreachable または Failed である場合、新規セルをデプロイできます。クラスタ内のセルの状態を表示するには、[データベースの高可用性クラスタ内のセルのステータスの表示](#) を参照してください。

このワークフローを使用することで、新しいスタンバイをデプロイするときに、障害が発生したスタンバイの IP アドレスとホスト名を再利用できます。

- 1 可能であれば、セル管理ツールを使用して vCloud Director プロセスをシャットダウンします。障害が発生したスタンバイ セルから次のコマンドを実行します。

```
/opt/vmware/vcloud-director/bin/cell-management-tool -u <admin username> cell --shutdown
```

- 2 障害が発生したスタンバイ仮想マシンをパワーオフします。
- 3 障害が発生したスタンバイ アプライアンスを、vCloud Director サーバ グループと repmgr 高可用性クラスタの両方から削除します。 [データベース高可用性クラスタ内の障害の発生したスタンバイ ノード、またはアクセスできないスタンバイ ノードの登録解除](#) を参照してください。
- 4 障害のあるスタンバイ セルの IP アドレスと DNS 名を再利用する場合は、障害のあるスタンバイをパワーオフ状態のままにするか、削除する必要があります。

- 5 新しいスタンバイ アプライアンスをデプロイします。[vCloud Director アプライアンスのデプロイの開始](#)ことも、[VMware OVF Tool を使用した vCloud Director アプライアンスのデプロイ](#)こともできます。

新しいスタンバイをデプロイした後に、クラスタの健全性は **健全** になっている必要があります。

## vCloud Director アプライアンスの組み込みデータベースのバックアップとリストア

vCloud Director アプライアンスの組み込み PostgreSQL データベースをバックアップして、障害発生後に vCloud Director 環境をリストアすることができます。

### vCloud Director アプライアンス組み込みデータベースのバックアップ

使用環境が組み込み PostgreSQL データベースを使用する vCloud Director アプライアンス展開で構成されている場合は、プライマリ セルから vCloud Director データベースをバックアップできます。作成された .tgz ファイルは、NFS 共有転送サービス ストレージの場所に保存されます。

#### 手順

- 1 プライマリ セルに root として直接ログインするか、SSH で接続します。
- 2 /opt/vmware/appliance/bin に移動します。
- 3 create-db-backup コマンドを実行します。

#### 結果

NFS 共有転送サービス ストレージの `vcloudapp.nfs_mount.VMware_vCloud_Director/pgdb-backup/` ディレクトリに、新しく作成された `db-backup-date_time_format.tgz` ファイルが表示されます。.tgz ファイルにはデータベース ダンプ ファイルと、プライマリ セルの `global.properties`、`responses.properties`、`certificates`、`proxycertificates`、および `truststore` ファイルが含まれています。

### 高可用性データベース構成の vCloud Director アプライアンス環境のリストア

高可用性データベース構成の vCloud Director アプライアンス環境に組み込まれた PostgreSQL データベースをバックアップした場合は、新しいアプライアンス クラスタをデプロイして、そこにアプライアンス データベースをリストアできます。

リストア ワークフローには、3 つの主要なステージがあります。

- 転送サービス NFS 共有ストレージから組み込みデータベースのバックアップ .tar ファイルをコピーする。
- 組み込みデータベースのプライマリおよびスタンバイ セルにデータベースをリストアする。
- 必要なアプリケーション セルをデプロイする。

#### 前提条件

- 組み込み PostgreSQL データベースの .tar ファイルがバックアップされていることを確認します。[vCloud Director アプライアンス組み込みデータベースのバックアップ](#)を参照してください。

- 1つのプライマリ データベース セルと 2つのスタンバイ データベース セルをデプロイします。『6 章 vCloud Director アプライアンスのデプロイ』を参照してください。
- 新しいアプライアンス クラスターで以前の環境の NFS サーバを使用する場合は、NFS サーバ上に新しい共有としてディレクトリを新規作成し、エクスポートします。既存のマウントポイントを再利用することはできません。

## 手順

- 1 プライマリ セルおよびスタンバイ セルで、root としてログインし、コマンドを実行して vCloud Director サービスを停止します。

```
service vmware-vcd stop
```

- 2 プライマリ セルおよびスタンバイ セルで、バックアップ .tar ファイルを /tmp フォルダにコピーします。  
/tmp フォルダに十分な空き容量がない場合は、別の場所を使用して .tar ファイルを保存します。
- 3 プライマリ セルおよびスタンバイ セルで、/tmp にあるバックアップ ファイルを解凍します。

```
tar -zxvf db-backup-date_time_format.tgz
```

/tmp フォルダに、抽出された global.properties、responses.properties、certificates、proxycertificates、truststore、およびデータベース ダンプ ファイル vcloud\_*date\_time\_format* が表示されます。

---

**注：** truststore ファイルは、vCloud Director 9.7.0.1 以降でのみ使用できます。

---

- 4 プライマリ セルのみで、root としてコンソールにログインし、以下のコマンドを実行します。
  - a vcloud データベースをドロップします。

```
sudo -i -u postgres /opt/vmware/vpostgres/current/bin/psql -c 'DROP DATABASE vcloud;'
```

- b pg\_restore コマンドを実行します。

```
sudo -i -u postgres /opt/vmware/vpostgres/current/bin/pg_restore -C -d postgres /tmp/  
vcloud_date_time_name
```

- 5 プライマリ セルおよびスタンバイ セルで、構成データ ファイルのコピーを保存し、置き換えてから、vCloud Director サービスを再構成して開始します。
  - a プロパティ、証明書、および truststore ファイルをバックアップします。

global.properties、responses.properties、certificates、proxycertificates、truststore の各ファイルは /opt/vmware/vcloud-director/etc/ にあります。

---

**注：** truststore ファイルは、vCloud Director 9.7.0.1 以降でのみ使用できます。

---

```
cd /opt/vmware/vcloud-director/etc  
mkdir -p backup  
cp global.properties responses.properties certificates proxycertificates truststore backup
```

- b [ステップ 3](#) で抽出したバックアップ ファイルから、プロパティ、証明書、truststore の各ファイルをコピーして置き換えます。

```
cd /tmp
cp global.properties responses.properties certificates proxycertificates truststore /opt/
vmware/vcloud-director/etc/.
```

**注：** truststore ファイルは、vCloud Director 9.7.0.1 以降でのみ使用できます。

```
cp certificates /opt/vmware/vcloud-director/.
```

- c /opt/vmware/vcloud-director/certificates.ks にあるキーストア ファイルをバックアップします。

```
cd /opt/vmware/vcloud-director
mkdir -p backup
cp certificates.ks backup
```

- d 以下のコマンドを実行して、vCloud Director サービスを再構成します。

```
/opt/vmware/vcloud-director/bin/configure --unattended-installation --database-type postgres
--database-user vcloud \
--database-password db_password_new_primary --database-host eth1_ip_new_primary --database-
port 5432 \
--database-name vcloud --database-ssl true --uuid --keystore /opt/vmware/vcloud-director/
certificates.ks \
--keystore-password ks_password --primary-ip appliance_eth0_ip \
--console-proxy-ip appliance_eth0_ip --console-proxy-port-https 8443
```

各値は次のとおりです。

- --keystore-password オプションは、アプライアンスの証明書のキーストア パスワードと一致します。
- --database-password オプションは、アプライアンスのデプロイ時に設定したデータベースのパスワードと一致します。
- --database-host オプションは、プライマリ データベース アプライアンスの eth1 ネットワーク IP アドレスと一致します。
- --primary-ip の値は、リストアするアプライアンス セルの eth0 ネットワーク IP アドレスと一致します。これは、プライマリ データベース セルの IP アドレスではありません。
- --console-proxy-ip オプションは、リストアするアプライアンス セルの eth0 ネットワーク IP アドレスと一致します。

トラブルシューティングの詳細については、[vCloud Director アプライアンスに移行またはリストアすると vCloud Director サービスの再構成に失敗する](#)を参照してください。

- e 以下のコマンドを実行して、vCloud Director サービスを開始します。

```
service vmware-vcd start
```



セルの起動の進行状況は `/opt/vmware/vcloud-director/logs/cell.log` で監視できます。

- 6 (オプション) 追加のアプリケーション セルをデプロイします。『[6 章 vCloud Director アプライアンスのデプロイ](#)』を参照してください。
- 7 サーバ グループのすべてのセルの起動プロセスが終了したら、vCloud Director 環境が正常にリストアしたことを確認します。
  - a 新しいサーバ グループ `https://et0_IP_new_cell/provider` 内の任意のセルの `eth0` ネットワーク IP アドレスを使用して、vCloud Director Service Provider Admin Portal を開きます。
  - b 既存のシステム管理者の認証情報を使用して、Service Provider Admin Portal にログインします。
  - c 新しい環境で vSphere およびクラウド リソースが使用可能であることを検証します。
- 8 データベースのリストアが成功したことを確認したら、Service Provider Admin Portal を使用して、古い vCloud Director 環境に属する切断されたセルを削除します。
  - a メイン メニュー (≡) から、[クラウド リソース] を選択します。
  - b 左側のパネルで [クラウド セル] をクリックします。
  - c 無効なセルを選択し、[登録解除] をクリックします。

## vCloud Director データベースへの外部アクセスの設定

特定の外部 IP アドレスからプライマリ アプライアンスに組み込まれた vCloud Director データベースへのアクセスを有効にできます。

vCloud Director アプライアンスへの移行中に、またはサードパーティのデータベース バックアップ ソリューションを使用している場合に、外部から組み込みの vCloud Director データベースへのアクセスを有効にすることができます。

### 手順

- 1 プライマリ セルに `root` として直接ログインするか、SSH で接続します。
- 2 データベース ディレクトリ `/opt/vmware/appliance/etc/pg_hba.d/` に移動します。
- 3 ターゲット外部 IP アドレスのエントリを含む、次のようなテキスト ファイルを作成します。

```
#TYPE DATABASE USER ADDRESS METHOD
host vcloud vcloud CIDR_notation md5
```

以下にその例を挙げます。

```
#TYPE DATABASE USER ADDRESS METHOD
host vcloud vcloud 172.168.100.5/32 md5
host vcloud vcloud 172.168.20.5/32 md5
```

エントリは、動的に更新される `pg_hba.conf` ファイルに追加されます。HA クラスタ内のプライマリ データベースへのアクセスは、このファイルによって制御されます。

## vCloud Director アプライアンスへの SSH アクセスの有効化または無効化

アプライアンスのデプロイ時、アプライアンスへの SSH アクセスは無効のままにすることも、有効にすることもできます。デプロイ後、SSH アクセスの設定を切り替えることができます。

SSH デーモンがアプライアンスで実行されるのは、データベース HA 機能に使用される場合と、リモートの root ログインの場合です。root ユーザーの SSH アクセスは、無効にすることができます。データベース HA 機能のための SSH アクセスは変更されません。

### 手順

- 1 テストなどの目的で、OVF プロパティを一時的に変更する場合は、vCloud Director のプロパティを変更します。
  - a vCloud Director アプライアンス コンソールに、root として直接ログインするか、SSH クライアントを使用して接続します。
  - b root による SSH アクセスを有効または無効にするためのスクリプトを実行します。
    - root による SSH アクセスを有効にするには、`/opt/vmware/appliance/bin/enable_root_login.sh` スクリプトを実行します。
    - root による SSH アクセスを無効にするには、`/opt/vmware/appliance/bin/disable_root_login.sh` スクリプトを実行します。
- 2 OVF プロパティを永続的に変更するには、vSphere ユーザー インターフェイスを使用して `vcloudapp.enable_ssh.VMware_vCloud_Director` プロパティの値を設定します。

---

**注：** vSphere のプロパティ値を変更するには、仮想マシンをパワーオフする必要があります。

---

- SSH を有効にするには、`vcloudapp.enable_ssh.VMware_vCloud_Director` の値を **True** に設定します。
- SSH を無効にするには、`vcloudapp.enable_ssh.VMware_vCloud_Director` の値を **False** に設定します。

## vCloud Director アプライアンスの DNS 設定の編集

デプロイ後に、vCloud Director アプライアンスの DNS サーバを変更できます。

---

**重要：** アプライアンスのホスト名は編集できません。新しいアプライアンスは目的のホスト名でデプロイする必要があります。

---

## 手順

- 1 テストなどの目的のために DNS 設定を一時的に変更する場合は、vCloud Director の DNS 設定を編集します。

- a vCloud Director アプライアンス コンソールに、root として直接ログインするか、SSH クライアントを使用して接続します。
- b (オプション) 次のコマンドを実行して、現在の DNS 構成を確認します。

```
ovfenv --key vami.DNS.VMware_vCloud_Director
```

- c DNS サーバを変更します。

複数の DNS サーバを指定するには、スペースを含まないカンマ区切りのリストとして *DNS\_server\_IP* を設定します。

```
ovfenv --key vami.DNS.VMware_vCloud_Director --value DNS_server_IP
```

- d 変更を有効にするには、VAOS サービスを再起動します。

```
systemctl restart vaos.service
```

- 2 DNS 設定を永続的に変更する場合は、vSphere ユーザー インターフェイスを使用して、*vami.DNS.VMware\_vCloud\_Director* プロパティの値を DNS サーバの新しい IP アドレスに設定します。

複数の DNS サーバを指定するには、スペースを含まないカンマ区切りのリストを入力します。

---

**注：** vSphere のプロパティ値を変更するには、仮想マシンをパワーオフする必要があります。

---

## vCloud Director アプライアンス ネットワーク インターフェイスのスタティック ルートの編集

最初の vCloud Director デプロイ後に、eth0 および eth1 ネットワーク インターフェイスのスタティック ルートを変更できます。

## 手順

- 1 テストなどの目的のためにスタティック ルートの値を一時的に変更する場合は、vCloud Director のスタティック ルートを編集します。

- a vCloud Director アプライアンス コンソールに、root として直接ログインするか、SSH クライアントを使用して接続します。
- b (オプション) 現在のスタティック ルート設定を確認します。

- eth0 については、次のコマンドを実行します。

```
ovfenv --key vcloudnet.routes0.VMware_vCloud_Director
```

- eth1 については、次のコマンドを実行します。

```
ovfenv --key vcloudnet.routes1.VMware_vCloud_Director
```

- c スタティック ルートの値を変更します。

スタティック ルートは、カンマ区切りリストの形式でルートを指定する必要があります。たとえば eth0 については、以下を実行する必要があります。

```
ovfenv --key vcloudnet.routes0.VMware_vCloud_Director --value "172.16.100.253  
172.16.96.0/19, 172.16.100.253 192.168.100.0/24"
```

- eth0 については、次のコマンドを実行します。

```
ovfenv --key vcloudnet.routes0.VMware_vCloud_Director --value "new_static_routes0"
```

- eth1 については、次のコマンドを実行します。

```
ovfenv --key vcloudnet.routes1.VMware_vCloud_Director --value "new_static_routes1"
```

- d vCloud Director アプライアンスでネットワーク サービスを再起動します。

```
systemctl restart vcd-ova-netconfig.service
```

- 2 スタティック ルートの値を永続的に変更する場合は、vSphere ユーザー インターフェイスを使用して、OVF プロパティを変更します。

スタティック ルートは、カンマ区切りリストの形式でルートを指定する必要があります。

---

**注：** vSphere のプロパティ値を変更するには、仮想マシンをパワーオフする必要があります。

---

- vSphere のユーザー インターフェイスを使用して、vcloudnet.routes0.VMware\_vCloud\_Director プロパティの値を新しいルート指定文字列に設定します。
- vSphere のユーザー インターフェイスを使用して、vcloudnet.routes1.VMware\_vCloud\_Director プロパティの値を新しいルート指定文字列に設定します。

## vCloud Director アプライアンスの構成スクリプト

vCloud Director アプライアンスには特定の構成スクリプトが含まれています。

ディレクトリ	説明
/opt/vmware/appliance/bin/	アプライアンス構成スクリプト。
/opt/vmware/appliance/etc/	アプライアンス構成ファイル。
/opt/vmware/appliance/etc/pg_hba.d/	pg_hba.conf ファイルにカスタム エントリを追加できるディレクトリ。 <a href="#">vCloud Director データベースへの外部アクセスの設定</a> を参照してください。

## vCloud Director アプライアンスの組み込み PostgreSQL データベースの容量の増加

vCloud Director アプライアンスの PostgreSQL データベース ディスクに十分な容量がない場合は、組み込みの PostgreSQL データベースの容量を増やすことができます。

PostgreSQL データベースは、ハード ディスク 3 に配置されています。デフォルト サイズは 80 GB です。この手順は、アプライアンスが動作している間に実行できます。

**重要：** プライマリ アプライアンスの容量を増やす前に、既存のスタンバイ アプライアンスの容量を増やす必要があります。

### 前提条件

- vCloud Director 環境にスタンバイ ノードがある場合は、スタンバイ ノードとプライマリ ノードを特定し、スタンバイ ノードから手順を開始します。ノードのロールの特定方法については、[データベース高可用性クラスタのステータスの確認](#)を参照してください。
- vCloud Director 環境がプライマリ ノードのみで構成されている場合は、プライマリ ノードでこの手順を実行します。

### 手順

- 1 vSphere Client にログインして、ハード ディスク 3 の容量を希望のサイズまで引き上げます。

各スタンバイ アプライアンスの PostgreSQL データベースのディスク サイズは、プライマリ アプライアンスの PostgreSQL データベース ディスクと同じサイズにする必要があります。

- a 変更するアプライアンス仮想マシンを選択します。
- b [アクション] - [設定の編集] の順に選択します。
- c [ハード ディスク 3] のサイズを大きくして、[OK] をクリックします。

再設定タスクの進行状況が、[最近のタスク] ペインに表示されます。

**2 データベースで使用されるボリュームの論理サイズを増やします。**

- a vCloud Director アプライアンス コンソールに、root として直接ログインするか、SSH クライアントを使用して接続します。
- b ハード ディスクのサイズ変更を OS に適用するには、次のコマンドを実行します。

```
echo 1 > /sys/class/scsi_device/2\:0\:2\:0/device/rescan
```

- c 物理ボリューム レイヤで認識される容量を正確に取得するには、次のコマンドを実行します。

```
pvresize /dev/sdc
```

- d (オプション) 次のコマンドを実行して、新しい物理ボリュームのサイズを確認します。

```
pvdisplay
```

- e 次のコマンドを実行して、論理ボリュームのサイズを変更します。

```
lvresize /dev/database_vg/vpostgres /dev/sdc
```

- f (オプション) 次のコマンドを実行して、新しい論理ボリュームのサイズを確認します。

```
lvdisplay
```

**3 ファイル システムのサイズを増やして、論理ボリューム全体が使用されるようにします。**

- a 追加容量を使用するには、次のコマンドを実行します。

```
resize2fs /dev/database_vg/vpostgres
```

- b (オプション) ファイル システムによって追加容量が使用されたことを確認するには、df -h を実行します。

追加容量は、OS で使用できます。システム出力は次のようになります。/dev/mapper/database\_vg-vpostgres 157G 75G 82G 48% /var/vmware/vpostgres

- 4 使用環境が1つのプライマリ アプライアンスのみで構成されているのではなく、他のスタンバイ ノードが含まれている場合は、データベースが配置されている他のすべてのスタンバイ ノードで手順1～3を繰り返してから、プライマリ ノードで手順1～3を繰り返します。

## vCloud Director アプライアンスでの PostgreSQL 設定の変更

vCloud Director アプライアンスの PostgreSQL の設定を変更するには、PostgreSQL の ALTER SYSTEM コマンドを使用します。

ALTER SYSTEM コマンドを実行すると、パラメータ設定の変更内容が postgresql.auto.conf ファイルに書き込まれます。PostgreSQL を初期化時には、このファイルが postgresql.conf ファイルよりも優先されます。設定によっては PostgreSQL サービスを再起動する必要がありますが、それ以外の設定は動的に構成されるため、再起動する必要はありません。postgresql.conf ファイルへの変更は再起動後には維持されないため、変更はしないでください。

## 手順

- 1 プライマリ アプライアンスの OS に root として直接ログインするか、SSH クライアントを使用して接続します。

- 2 ユーザーを postgres に変更します。

```
sudo -i -u postgres
```

- 3 PostgreSQL ALTER SYSTEM コマンドを使用して、パラメータを変更します。

```
psql -c "ALTER SYSTEM set parameter='value';"
```

- 4 変更する構成パラメータごとに [手順 3](#) を繰り返します。

- 5 変更するパラメータの中に PostgreSQL サービスの再起動を要求するものがある場合は、vpostgres プロセスを再起動します。

```
systemctl restart vpostgres
```

- 6 使用環境内にスタンバイ ノードがある場合は、postgresql.auto.conf ファイルをスタンバイ アプライアンスにコピーし、必要に応じて PostgreSQL サービスを再起動します。

- a プライマリ ノードからスタンバイ ノードに postgresql.auto.conf ファイルをコピーします。

```
scp /var/vmware/vpostgres/current/pgdata/postgresql.auto.conf postgres@<standby-node-address>:/var/vmware/vpostgres/current/pgdata/
```

- b コピーした postgresql.auto.conf ファイル内の一部のパラメータを有効にするために再起動する必要がある場合は、スタンバイ ノードで vpostgres プロセスを再起動します。

```
systemctl restart vpostgres
```

- c スタンバイ ノードごとに [6.a](#) および [6.b](#) を繰り返します。

# 高可用性クラスタ構成でのレプリケーション マネージャ ツール スイートの使用

## 9

repmgr オープン ソースのツール スイートは、vCloud Director アプライアンスの組み込み PostgreSQL データベースに含まれています。repmgr を使用して、vCloud Director データベース高可用性クラスタで PostgreSQL レプリケーションおよびデータベース フェイルオーバーを設定、監視、制御することができます。

repmgr コマンドライン インターフェイスを使用して、ノードまたはクラスタのステータスとイベントの確認、ノードの登録または登録解除、スタンバイ ノードの昇格、プライマリとスタンバイのロールのスワップ、または新しいプライマリ ノードへの準拠を行うことができます。

vCloud Director データベースの高可用性構成の詳細については、[アプライアンス環境とデータベースの高可用性構成](#)を参照してください。

repmgr の詳細については、[repmgr.org](http://repmgr.org) を参照してください。

この章には、次のトピックが含まれています。

- [データベース高可用性クラスタの接続ステータスの確認](#)
- [データベース高可用性クラスタのノードのレプリケーション ステータスの確認](#)
- [データベース高可用性クラスタのステータスの確認](#)
- [高可用性クラスタでオンラインに復帰した以前のプライマリ ノードの検出](#)
- [データベース高可用性クラスタ内のプライマリ セルおよびスタンバイ セルのロールの切り替え](#)
- [データベース高可用性クラスタ内の障害の発生したスタンバイ ノード、またはアクセスできないスタンバイ ノードの登録解除](#)
- [データベース高可用性クラスタ内の障害の発生したプライマリ セルの登録解除](#)
- [データベース高可用性クラスタ内の実行中のスタンバイ セルの登録解除](#)

## データベース高可用性クラスタの接続ステータスの確認

レプリケーション マネージャ ツール スイートを使用して、データベース高可用性クラスタ内のノード間の接続を確認できます。

### 手順

- 1 クラスタで実行されているいずれかのセルの OS に、**root** としてログインするか、SSH で接続します。



## 2 ユーザーを **postgres** に変更します。

```
sudo -i -u postgres
```

## 3 クラスタの接続を確認します。

- `repmgr cluster matrix` コマンドはクラスタの各ノードで `repmgr cluster show` コマンドを実行し、結果をマトリックスとして表示します。

```
/opt/vmware/vpostgres/current/bin/repmgr -f /opt/vmware/vpostgres/current/etc/repmgr.conf
cluster matrix
```

次の例では、ノード 1 とノード 2 は稼動中であり、ノード 3 は停止しています。各行は 1 つのサーバに対し、そのサーバからの送信接続のテスト結果を表しています。

3 行目の 3 つのエントリには ? 記号が付いています。これは、ノード 3 が停止しており、送信接続に関する情報がいないためです。

Name	Id	1	2	3
node 1	1	*	*	x
node 2	2	*	*	x
node 3	3	?	?	?

- `repmgr cluster crosscheck` コマンドを実行すると、ノードの各組み合わせ間の接続が照合され、クラスタ接続の概要を確認できることがあります。

```
/opt/vmware/vpostgres/current/bin/repmgr -f /opt/vmware/vpostgres/current/etc/repmgr.conf
cluster crosscheck
```

次の例では、`repmgr cluster crosscheck` コマンドの実行元のノードでクラスタ マトリックス システムからの出力と他のノードからの出力がマージされて、ノード間の照合が行われます。この場合、すべてのノードが稼動していますが、ファイアウォールはノード 1 から送信されたパケットをドロップし、ノード 3 に転送します。これは、ノード 1 がパケットをノード 3 に送信できない、非対称的なネットワーク パーティションの例です。

Name	Id	1	2	3
node 1	1	*	*	x
node 2	2	*	*	*
node 3	3	*	*	*

### 次のステップ

データベース高可用性クラスタの全体的な接続ステータスを確認するには、各ノードでこれらのコマンドを実行し、結果を比較します。

## データベース高可用性クラスタのノードのレプリケーション ステータスの確認

レプリケーション マネージャ ツール スイートおよび PostgreSQL インタラクティブ ターミナルを使用して、データベース高可用性クラスタ内の個別のノードのレプリケーション ステータスを確認できます。

### 手順

- 1 クラスタで実行されているいずれかのノードの OS に、**root** としてログインするか、SSH で接続します。
- 2 ユーザーを **postgres** に変更します。

```
sudo -i -u postgres
```

- 3 ノードのレプリケーション ステータスを確認します。

```
/opt/vmware/vpostgres/current/bin/repmgr -f /opt/vmware/vpostgres/current/etc/repmgr.conf node status
```

システム出力には、ノード、PostgreSQL のバージョン、およびレプリケーションの詳細に関する情報が示されます。

- 4 (オプション) 詳細については、PostgreSQL インタラクティブ ターミナルを使用してノードのレプリケーション ステータスを確認してください。

PostgreSQL インタラクティブ ターミナルでは、スタンバイ ノードで受信したログ レコードの中に、プライマリから送信されたログよりも遅延しているものがあるかどうかに関する情報を提供できます。

- a **psql** ターミナルに接続します。

```
/opt/vmware/vpostgres/current/bin/psql
```

- b 表示を拡張してクエリ結果を読みやすくするには、**set \x** コマンドを実行します。
- c ノードのロールに応じて、レプリケーション ステータスに関するクエリを実行します。

オプション	アクション
プライマリ ノードでクエリを実行します。	<code>/opt/vmware/vpostgres/current/bin/psql</code>
スタンバイ ノードでクエリを実行します。	<code>select * from pg_stat_wal_receiver;</code>

## データベース高可用性クラスタのステータスの確認

データベース高可用性クラスタの問題のトラブルシューティングを行うには、クラスタ内のノードおよびイベントのステータスを監視する必要があります。

### 手順

- 1 クラスタで実行されているいずれかのセルの OS に、**root** としてログインするか、SSH で接続します。

## 2 ユーザーを **postgres** に変更します。

```
sudo -i -u postgres
```

## 3 クラスタのステータスを確認します。

[アップストリーム] 列には、現在のプライマリ ノードが表示されます。

```
/opt/vmware/vpostgres/current/bin/repmgr cluster show
```

コンソール出力に、クラスタの情報が表示されます。次の例では、クラスタのプライマリ ノード（ノード 3）にアクセスできません。

ID	Name	Role	Status	Upstream	Location	Connection string
Node 1	<i>Node name</i>	standby	running	<i>Node 3 name</i>	default	host= <i>host IP address</i> user=repmgr dbname=repmgr
Node 2	<i>Node name</i>	standby	running	<i>Node 3 name</i>	default	host= <i>host IP address</i> user=repmgr dbname=repmgr
Node 3	<i>Node name</i>	primary	? unreachable		default	host= <i>host IP address</i> user=repmgr dbname=repmgr

次のシステム出力例では、ノード 3 は正常に動作しているクラスタ内のプライマリ ノードです。

ID	Name	Role	Status	Upstream	Location	Connection string
Node 1	<i>Node name</i>	standby	running	<i>Node3 name</i>	default	host= <i>host IP address</i> user=repmgr dbname=repmgr
Node 2	<i>Node name</i>	standby	running	<i>Node3 name</i>	default	host= <i>host IP address</i> user=repmgr dbname=repmgr
Node 3	<i>Node name</i>	primary	*running		default	host= <i>host IP address</i> user=repmgr dbname=repmgr

## 4 クラスタのイベント ログを確認します。

```
/opt/vmware/vpostgres/current/bin/repmgr -f /opt/vmware/vpostgres/current/etc/repmgr.conf cluster event
```

システム出力には、クラスタ内の作成、クローン作成、および登録のイベントが表示されます。

### 次のステップ

プライマリ ノードのステータスが **Unreachable** または **Failed** である場合は、スタンバイ ノードを昇格する必要があります。

スタンバイノードのステータスが **Unreachable** または **Failed** である場合は、ノードを修復し、PostgreSQL サービスが実行されていない場合は、これを起動します。

## 高可用性クラスタでオンラインに復帰した以前のプライマリ ノードの検出

クラスタ内のプライマリ ノードに障害が発生して、スタンバイ ノードを新しいプライマリに昇格してから、プライマリ ノードがオンラインに戻った場合は、repmgr データが不正確になります。不正な設定は、repmgr cluster show コマンドで検出できます。

### 例：以前のプライマリ ノードで repmgr cluster show を実行する

次の例では、オンラインに復帰した以前のプライマリ ノードで repmgr cluster show コマンドを実行すると、次のようなシステム出力が生成されます。

```

      ID | Name      | Role   | Status           | Upstream | Location | Connection string
-----+-----+-----+-----+-----+-----+-----
Node 1 | Node1 name | standby | !running as primary | Node 3 name | default | host=host IP address
user=repmgr dbname=repmgr
Node 2 | Node2 name | standby | running          | Node 3 name | default | host=host IP address
user=repmgr dbname=repmgr
Node 3 | Node3 name | primary | * running        |           | default | host=host IP address
user=repmgr dbname=repmgr
WARNING: following issues were detected
- node 1(ID: Node 1) is registered as standby but running as primary

```

この例では、ノード 1 がクラスタ内の現在のプライマリ ノードです。

repmgr cluster show コマンドを実行するときに、スタンバイ ノードの !running as primary ステータスが取得された場合は、以前のプライマリ ノードがクラスタ内で実行されていることを意味します。この場合は、以前のプライマリ ノードをシャットダウンして登録解除する必要があります。

### 例：新しいプライマリで repmgr cluster show を実行する

次の例では、新しいプライマリ ノードで repmgr cluster show コマンドを実行すると、次のようなシステム出力が生成されます。

```

      ID | Name      | Role   | Status           | Upstream | Location | Connection string
-----+-----+-----+-----+-----+-----+-----
Node 1 | Node1 name | primary | * running        |           | default | host=host IP address user=repmgr
dbname=repmgr
Node 2 | Node2 name | standby | running          | Node1 name | default | host=host IP address user=repmgr
dbname=repmgr
Node 3 | Node3 name | primary | ! running        |           | default | host=host IP address user=repmgr
dbname=repmgr
WARNING: following issues were detected
- node 3(ID: Node 3) is running but the repmgr node record is inactive

```

この場合、repmgr データは正確です。ノード 1 が実行されていて、現在のプライマリ ノードであることを正確に示しています。ノード 3（以前のプライマリ）に関する警告メッセージは、このノードの repmgr データが正確でないことを示します。

## 例：スタンバイ ノードの昇格後、残りのスタンバイ ノードで standby follow を実行せずに repmgr cluster show を実行する

次の例では、プライマリ ノードに障害が発生したクラスタ内のノードごとに、repmgr データを表示できます。repmgr standby promote コマンドを使用してスタンバイを手動で昇格しましたが、残りのスタンバイ ノードで repmgr standby follow を実行していません。

新しいプライマリで repmgr cluster show を実行すると、システム出力は正しい repmgr データを表しますが、新しいプライマリ ノード（ノード 2）の後ろにはスタンバイ ノードがありません。

```

      ID | Name      | Role   | Status      | Upstream | Location | Connection string
-----+-----+-----+-----+-----+-----+-----
Node 1 |Node1 name| primary | * running |          | default | host=host IP address user=repmgr
dbname=repmgr
Node 2 |Node2 name| primary | ! running |          | default | host=host IP address user=repmgr
dbname=repmgr
Node 3 |Node3 name| standby | running |Node 1 name| default | host=host IP address user=repmgr
dbname=repmgr
WARNING: following issues were detected
- node 1(ID: Node 1) is running but the repmgr node record is inactive

```

以前のプライマリであるノード 1 と、以前のプライマリの後ろにありスタンバイであるノード 3 の両方が、不正確な repmgr データを提供します。

```

      ID | Name      | Role   | Status      | Upstream | Location | Connection string
-----+-----+-----+-----+-----+-----+-----
Node 1 |Node1 name| primary | * running |          | default | host=host IP address
user=repmgr dbname=repmgr
Node 2 |Node2 name| standby | ! running as primary |Node1 name| default | host=host IP address
user=repmgr dbname=repmgr
Node 3 |Node3 name| standby | running |Node1 name| default | host=host IP address
user=repmgr dbname=repmgr
WARNING: following issues were detected
- node 2(ID: Node 2) is registered as standby but running as primary

```

## 例：スタンバイ ノードで repmgr cluster show を実行する

現在のプライマリの後ろにあるスタンバイ ノードでコマンドを実行すると、現在のプライマリのデータと同一の正確な repmgr データを含むシステム出力が生成されます。

以前のプライマリの後ろにあるスタンバイ ノードでコマンドを実行すると、以前のプライマリのデータと同一の不正確な repmgr データを含むシステム出力が生成されます。

## ログ エントリ

スタンバイ ノードを新しいプライマリに昇格した後に、障害が発生した以前のプライマリがオンラインに戻った場合は、すべてのノード上の `update-repmgr-data.log` ファイルに、不正確な repmgr データを含む次のエントリが表示されます。

```
ERROR: An old primary is running in the repmgr cluster.
ERROR: Manual intervention is required to repair the repmgr cluster.
ERROR: The first step should be to shutdown and unregister the old primary.
```

## データベース高可用性クラスタ内のプライマリ セルおよびスタンバイ セルのロールの切り替え

repmgr コマンドを使用して、計画メンテナンス時に、データベース高可用性クラスタ内のプライマリ ノードのロールとスタンバイ ノードのロールを切り替えることができます。

### 前提条件

- 高可用性クラスタに含まれるすべての vCloud Director セルをメンテナンス モードに切り替えます。
- クラスタ内のすべてのノードが健全で、オンラインになっていることを確認します。

### 手順

- 1 昇格するスタンバイ ノードの OS に **root** としてログインするか、SSH で接続します。
- 2 ユーザーを **postgres** に変更します。

```
sudo -i -u postgres
```

- 3 (オプション) `--dry-run` オプションを指定して次のコマンドを実行し、切り替えの前提条件が満たされていることを確認します。

```
/opt/vmware/vpostgres/current/bin/repmgr standby switchover -f /opt/vmware/vpostgres/current/etc/repmgr.conf --siblings-follow --dry-run
```

- 4 プライマリ セルおよびスタンバイ セルのロールを切り替えます。

```
/opt/vmware/vpostgres/current/bin/repmgr standby switchover -f /opt/vmware/vpostgres/current/etc/repmgr.conf --siblings-follow
```

### 結果

コンソール出力の最後の行は、スタンバイの切り替えが正常に完了したことを示します。

### 次のステップ

- 1 **reconfigure-database** コマンドを実行して、すべての vCloud Director セルのデータベース IP アドレスを更新します。[vCloud Director セルのデータベース IP アドレスの更新](#)を参照してください。

- 2 新しいプライマリ データベースを参照するようにサーバ グループ内の vCloud Director セルを再設定する場合は、高可用性クラスタに含まれているすべての vCloud Director セルのメンテナンス モードを解除します。

## データベース高可用性クラスタ内の障害の発生したスタンバイ ノード、またはアクセスできないスタンバイ ノードの登録解除

クラスタの実行中のノードに repmgr を使用すると、障害の発生したスタンバイ ノード、またはアクセスできないスタンバイ ノードを登録解除できます。

**注：** プライマリ ノードが正常に機能するようにするには、1 台以上のスタンバイ ノードが常に実行されている必要があります。

### 前提条件

実行されていないスタンバイ ノードを登録解除するには、ノード ID を指定する必要があります。IP アドレスを見つけるには、クラスタのステータスを確認して、ノードを特定します。この行の Connection string 列のホスト値を使用してノードの IP アドレスを特定します。[データベース高可用性クラスタのステータスの確認](#)を参照してください。

### 手順

- 1 クラスタで実行されているいずれかのノードの OS に、**root** としてログインするか、SSH で接続します。
- 2 ユーザーを **postgres** に変更します。

```
sudo -i -u postgres
```

- 3 障害の発生したノードまたはアクセスできないノードを登録解除します。

```
/opt/vmware/vpostgres/current/bin/repmgr standby unregister -f /opt/vmware/vpostgres/current/etc/repmgr.conf --node-id=ID
```

### 結果

ノードを登録解除すると、repmgr メタデータからノード情報が削除されます。

## データベース高可用性クラスタ内の障害の発生したプライマリ セルの登録解除

データベース高可用性クラスタのプライマリ ノードで障害が発生し、新しいプライマリを昇格する場合は、障害が発生したプライマリ ノードを登録解除し、クラスタから削除して、クラスタ ステータスのデータの不整合な状態を回避します。

### 前提条件

- 実行されていないプライマリ ノードを登録解除するには、ノード ID を指定する必要があります。IP アドレスを見つけるには、クラスタのステータスを確認して、ノードを特定します。この行の Connection string 列のホスト値を使用してノードの IP アドレスを特定します。[データベース高可用性クラスタのステータスの確認](#)を参照してください。
- 障害が発生したプライマリが、非アクティブになっていて、次のスタンバイ ノードがないことを確認して、新しいプライマリを昇格します。

### 手順

- 1 クラスタで実行されているいずれかのノードの OS に、**root** としてログインするか、SSH で接続します。
- 2 ユーザーを **postgres** に変更します。

```
sudo -i -u postgres
```

- 3 (オプション) ノードの登録解除の前提条件が満たされていることを確認するには、**--dry-run** オプションを指定して次のコマンドを実行します。

```
/opt/vmware/vpostgres/current/bin/repmgr primary unregister --node-id=node ID --dry-run
```

- 4 ノードを登録解除します。

```
/opt/vmware/vpostgres/current/bin/repmgr primary unregister --node-id=node ID
```

### 結果

この操作を行うと、repmgr メタデータからノードが削除されます。

## データベース高可用性クラスタ内の実行中のスタンバイ セルの登録解除

別のロールのノードを使用する場合、または高可用性クラスタからノードを削除する場合は、そのノードを登録解除する必要があります。

このコマンドは、通常のシステム運用中に実行できます。

**注：** プライマリ ノードが正常に機能するようにするには、1 台以上のスタンバイ ノードが常に行動している必要があります。

### 前提条件

スタンバイ ノードを登録解除するには、ノード ID を指定する必要があります。IP アドレスを見つけるには、クラスタのステータスを確認して、ノードを特定します。この行の Connection string 列のホスト値を使用してノードの IP アドレスを特定します。[データベース高可用性クラスタのステータスの確認](#)を参照してください。

### 手順

- 1 クラスタで実行されているいずれかのノードの OS に、**root** としてログインするか、SSH で接続します。



## 2 ユーザーを **postgres** に変更します。

```
sudo -i -u postgres
```

## 3 ノードを登録解除します。

```
/opt/vmware/vpostgres/current/bin/repmgr standby unregister --node-id=node ID -f /opt/vmware/  
vpostgres/current/etc/repmgr.conf
```

### 結果

ノードを登録解除すると、repmgr ツールスイートの内部メタデータ テーブルからスタンバイのレコードが削除されます。

# セル管理ツール リファレンス

# 10

セル管理ツールは、vCloud Director セルまたはデータベースの管理に使用するコマンド ライン ユーティリティです。大半の操作には、スーパーユーザーまたはシステム管理者の認証情報が必要です。

セル管理ツールは、`/opt/vmware/vcloud-director/bin/` にインストールされます。これは、単一のコマンドの実行またはインタラクティブ シェルとして実行する場合に使用できます。

## 使用可能なコマンドの一覧表示

使用可能なセル管理ツールのコマンドを一覧表示するには、次のコマンドラインを使用します。

```
./cell-management-tool -h
```

## シェル モードの使用

セル管理ツールは、ここに示されているように引数なしで呼び出すことによって、インタラクティブ シェルとして実行できます。

```
[root@cell1 /opt/vmware/vcloud-director/bin]#./cell-management-tool  
セル管理ツール v8.14.0.4146350。利用可能なサブコマンドについては、「help」と入力してください。cmt>
```

シェル モードでは、次の例に示されているように、`cmt>` プロンプトでセル管理ツールの任意のコマンドを入力できます。

```
cmt>cell -h  
usage: cell [options] -a,--application-states display the state of each application on the cell  
[DEPRECATED - use the cell-application command instead] -h,--help print this message -i,--pid <arg>  
the process id of the cell [REQUIRED if username is not specified] -m,--maintenance <arg> gracefully  
enter maintenance mode on the cell -p,--password <arg> administrator password [OPTIONAL] -q,--quiesce  
<arg> quiesce activity on the cell -s,--shutdown gracefully shutdown the cell -t,--status display  
activity on the cell -tt,--status-verbose display a verbose description of activity on the cell -u,--  
username <arg> administrator username [REQUIRED if pid is not specified] Note: You will be prompted  
for administrator password if not entered in command line. cmt>
```

実行が終了すると、コマンドは `cmt>` プロンプトに戻ります。シェル モードを終了するには、`cmt>` プロンプトで **exit** と入力します。

## 例：セル管理ツールの使用法のヘルプ

この例では、使用可能なシェル管理ツールのコマンドをリストする単一の非インタラクティブ コマンドを実行しています。

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./cell-management-tool -h
usage: cell-management-tool -h,--help print this message Available commands: cell - Manipulates the
Cell and core components certificates - Reconfigures the SSL certificates for the cell . . . For
command specific help: cell-management-tool <commandName> -h
```

### ■ vCloud Director インストール環境の構成

サーバ グループのデータベースをシステム管理者のアカウントと関連情報で初期化するには、セル管理ツールの `system-setup` コマンドを使用します。

### ■ vCloud Director Web Console の有効化

vCloud Director 10.0 では、vCloud Director Web Console (Flex ベース ユーザー インターフェイス) は廃止されていて、デフォルトで無効になっています。Web Console URL は、サービス プロバイダおよびテナントの対応する HTML5 トップ ページにリダイレクトします。セル管理ツールを使用して、Web Console を有効にできます。

### ■ レガシー API エンドポイントへのサービス プロバイダ アクセスの無効化

vCloud Director 10.0 以降では、サービス プロバイダおよびテナントから vCloud Director へのアクセスに、個別の vCloud Director OpenAPI ログイン エンドポイントを使用できます。

### ■ セルの管理

セル管理ツールの `cell` サブコマンドを使用すると、タスク スケジューラをサスペンドして新しいタスクを開始できないようにしたり、アクティブなタスクのステータスを表示したり、セルのメンテナンス モードをコントロールしたり、セルを正常にシャットダウンしたりすることができます。

### ■ セル アプリケーションの管理

セルの起動時に実行される一連のアプリケーションを管理するには、セル管理ツールの `cell-application` コマンドを使用します。

### ■ データベース接続プロパティを更新する

セル管理ツールの `reconfigure-database` サブコマンドを使用すると、vCloud Director データベースの接続プロパティを更新できます。

### ■ 破損したスケジューラ データの検出および修復

vCloud Director は、クォーツ ジョブ スケジューラを使用して、システムで実行されている非同期操作 (ジョブ) を連携します。クォーツ スケジューラ データベースが破損すると、システムを正常に静止できない場合があります。スケジューラ データの破損の有無を確認するには、セル管理ツールの `fix-scheduler-data` コマンドを使用して、データベースをスキャンします。データが破損していた場合は、必要に応じて修復します。

### ■ HTTP およびコンソール プロキシ エンドポイントの自己署名証明書の生成

セル管理ツールの `generate-certs` コマンドを使用して、HTTP およびコンソール プロキシ エンドポイントの自己署名付き SSL 証明書を生成します。

- [HTTP およびコンソール プロキシ エンドポイントの証明書の置き換え](#)

セル管理ツールの `certificates` コマンドを使用して、HTTP およびコンソール プロキシ エンドポイントの SSL 証明書を置き換えます。

- [外部サービスからの SSL 証明書のインポート](#)

セル管理ツールの `import-trusted-certificates` コマンドを使用して、AMQP や vCloud Director データベースなどの外部サービスへのセキュアな接続の確立に使用する証明書をインポートします。

- [許可された SSL 暗号のリストの管理](#)

SSL ハンドシェイク プロセス中に使用するためにセルが提供する暗号化スイートのセットを構成するには、セル管理ツールの `ciphers` コマンドを使用します。

- [許可された SSL プロトコルのリストの管理](#)

SSL ハンドシェイク プロセス中にセルが使用を提案する SSL プロトコルのセットを構成するには、セル管理ツールの `ssl-protocols` コマンドを使用します。

- [メトリック収集の設定](#)

セル管理ツールの `configure-metrics` コマンドを使用して、収集するメトリックのセットを設定します。

- [Cassandra メトリック データベースの構成](#)

セルをオプションのメトリック データベースに接続するには、セル管理ツールの `cassandra` コマンドを使用します。

- [システム管理者のパスワードの復元](#)

vCloud Director データベースのユーザー名とパスワードが分かっている場合は、セル管理ツールの `recover-password` コマンドを使用して、vCloud Director システム管理者のパスワードを復元できます。

- [タスクの失敗ステータスの更新](#)

セルが意図的にシャットダウンされたときに実行していたタスクに関連する完了ステータスを更新するには、セル管理ツールの `fail-tasks` コマンドを使用します。すべてのセルをシャットダウンしない限り、`fail-tasks` コマンドを使用することはできません。

- [監査メッセージ処理の構成](#)

システムが監査メッセージをログに記録する方法を構成するには、セル管理ツールの `configure-audit-syslog` コマンドを使用します。

- [電子メール テンプレートの構成](#)

電子メール アラートを作成する際にシステムが使用するテンプレートを管理するには、セル管理ツールの `manage-email` コマンドを使用します。

- [親なしの仮想マシンの検索](#)

セル管理ツールの `find-orphan-vms` コマンドを使用すると、vCenter データベースには存在するが vCloud Director データベースには存在しない仮想マシンへの参照を検索できます。

- [VMware カスタマ エクスペリエンス改善プログラムへの参加または離脱](#)

VMware カスタマ エクスペリエンス改善プログラムに参加または離脱するには、セル管理ツールの `configure-ceip` サブコマンドを使用します。

## ■ アプリケーションの設定の更新

セル管理ツールの `manage-config` サブコマンドを使用すると、カタログ スロットリング アクティビティなどのさまざまなアプリケーションの構成を更新できます。

## ■ カタログ同期のスロットリングの設定

他の組織に公開された、または他の組織からサブスクライブされたカタログ項目が多数ある場合、カタログの同期中にシステムが過負荷にならないように、カタログ同期のスロットリングを設定できます。セル管理ツールの `manage-config` サブコマンドを使用すると、同時に同期できるライブラリ項目の数を制限することで、カタログ同期のスロットリングを設定できます。

## ■ vCloud Director ユーザー インターフェイスへのアクセスに失敗した場合のトラブルシューティング

vCloud Director 環境内の vCloud Director セルの有効な IP アドレスと DNS エントリを表示および更新するには、セル管理ツールの `manage-config` サブコマンドを使用します。

## ■ vCenter Server 仮想マシン検出のデバッグ

セル管理ツールの `debug-auto-import` サブコマンドを使用すると、vApp の検出メカニズムが vCenter Server 仮想マシンを 1 台以上スキップする原因を調査できます。

## ■ マルチサイト拡張ネットワークの MAC アドレスの再生成

同じインストール ID で構成されている 2 つの vCloud Director サイトを関連付けると、これらのサイト間の拡張ネットワークで MAC アドレスの競合が発生する可能性があります。このような競合を回避するには、インストール ID とは異なるカスタム シードに基づいて、いずれかのサイトで MAC アドレスを再生成する必要があります。

## ■ vCloud Director セルのデータベース IP アドレスの更新

セル管理ツールを使用して、データベース高可用性クラスタ内の vCloud Director セルの IP アドレスを更新できます。

# vCloud Director インストール環境の構成

サーバ グループのデータベースをシステム管理者のアカウントと関連情報で初期化するには、セル管理ツールの `system-setup` コマンドを使用します。

vCloud Director サーバ グループに属するすべてのサーバを構成し、データベースに接続したら、最初のシステム管理者アカウントを作成し、次の形式のコマンド ラインを使用して vCloud Director データベースを関連情報で初期化できます。

```
cell-management-tool system-setup options
```

このコマンドを、セットアップ済みのシステムで実行することはできません。 `--unattended` と `--password` を除くすべてのオプションを指定する必要があります。

表 10-1. セル管理ツールのオプションと引数、system-setup サブコマンド

オプション	引数	説明
--help (-h)	なし	このカテゴリで使用可能なコマンドの概要を示します。
--email	作成するシステム管理者のメール アドレス。	システム管理者のメール アドレスは、vCloud Director データベースに格納されます。
--full-name	作成するシステム管理者のフル ネーム。	システム管理者のフル ネームは、vCloud Director データベースに格納されます。
--installation-id	1 ～ 63 の整数	<p>この vCloud Director インストール環境のインストール ID。このインストール ID は、仮想 NIC の MAC アドレスを生成する際に使用されます。</p> <p><b>注：</b> マルチサイト展開の vCloud Director インストール間で拡張ネットワークを作成する予定がある場合は、各 vCloud Director インストールに一意的インストール ID を設定することを検討してください。</p>
--password	作成するシステム管理者のパスワード。 --unattended オプションを使用する場合は必須です。--unattended オプションを使用していない場合に、コマンドラインにこのオプションを指定しないと、パスワードを尋ねるプロンプトが表示されます。	システム管理者は、vCloud Director の認証を受ける際に、このパスワードを入力します。
--serial-number	このインストールのシリアル番号 (ライセンス キー)。	任意。vCloud Director の有効なシリアル番号であることが必要です。
--system-name	vCloud Director vCenter Server フォルダの名前。	この vCloud Director インストール環境は、登録先の各 vCenter Server で、この名前のフォルダによって表されます。
--unattended	なし	任意。このオプションを指定してコマンドを起動すると、入力を求めるプロンプトが表示されなくなります。
--user	作成するシステム管理者のユーザー名。	システム管理者は、vCloud Director の認証を受ける際に、このユーザー名を入力します。

## 例： vCloud Director システム設定を指定する

この例のコマンドでは、vCloud Director インストール環境に必要なすべてのシステム設定を指定しています。--unattended および --password オプションが指定されていないため、システム管理者を作成する際にパスワードを入力および確認するよう要求されます。

```
[root@cell1 /opt/vmware/vcloud-director/
bin]#./cell-management-tool system-setup \ --user admin --full-name "VCD System Administrator" --
email vcd-admin@example.com --system-name VCD --installation-id 2
Please enter the new password for user admin (password must have more than 6 characters):

Re-enter the password to confirm:

Username: admin
Full name: VCD System Administrator
Email: vcd-admin@example.com
System name: VCD
Installation ID: 2
Are you sure you want to use these parameters? [Y/n]:y
Creating admin user.
Setting system details.
Completing system setup.
System setup is complete.
```

## vCloud Director Web Console の有効化

vCloud Director 10.0 では、vCloud Director Web Console (Flex ベース ユーザー インターフェイス) は廃止されていて、デフォルトで無効になっています。Web Console URL は、サービス プロバイダおよびテナントの対応する HTML5 トップ ページにリダイレクトします。セル管理ツールを使用して、Web Console を有効にできます。

### 手順

- 1 いずれかの vCloud Director セルの OS に、**root** としてログインするか、SSH で接続します。
- 2 セル管理ツールを使用して Web Console を有効にします。

- すべてのユーザーに対して Web Console を有効にするには、次のコマンドを実行します。

```
/opt/vmware/vcloud-director/bin/cell-management-tool manage-config -n flex.ui.enabled -v true
```

- Web Console をシステム管理者に対してのみ有効にするには、次のコマンドを実行します。

```
/opt/vmware/vcloud-director/bin/cell-management-tool manage-config -n flex.ui.enabled -v sys-
admin-only
```

表 10-2. セル管理ツールのオプションと引数、manage-config サブコマンド

オプション	引数	説明
--name(-n)	flex.ui.enabled	Web Console を有効または無効にするフラグ。
--value(-v)	false (デフォルト)	<p>引数 false は Web Console を無効にします。これがデフォルトの動作です。</p> <ul style="list-style-type: none"> <li>■ <i>base_cell_URL/</i> - リダイレクトせずにログイン ページを再ロードします。</li> <li>■ <i>base_cell_URL/cloud - /</i> provider にリダイレクトします。</li> <li>■ <i>base_cell_URL/cloud/login.jsp - /</i> provider にリダイレクトします。</li> <li>■ <i>base_cell_URL/cloud/org/organization_name - /tenant/organization_name</i> にリダイレクトします。</li> </ul>
	true	<p>引数 true は Web Console を有効にします。</p> <ul style="list-style-type: none"> <li>■ <i>base_cell_URL/</i> - リダイレクトせずにログイン ページを再ロードします。</li> <li>■ <i>base_cell_URL/cloud</i> - リダイレクトしません。</li> <li>■ <i>base_cell_URL/cloud/login.jsp</i> - リダイレクトしません。</li> <li>■ <i>base_cell_URL/cloud/org/organization_name</i> - リダイレクトしません。</li> </ul>
	sys-admin-only	<p>引数 sys-admin-only はシステム管理者に対して Web Console を有効にします。</p> <ul style="list-style-type: none"> <li>■ <i>base_cell_URL/</i> - リダイレクトせずにログイン ページを再ロードします。</li> <li>■ <i>base_cell_URL/cloud</i> - リダイレクトしません。</li> <li>■ <i>base_cell_URL/cloud/login.jsp</i> - リダイレクトしません。</li> <li>■ <i>base_cell_URL/cloud/org/organization_name - /tenant/organization_name</i> にリダイレクトします。</li> </ul>

### 3 vCloud Director セルを再起動して、この変更を有効にします。

```
service vmware-vcd restart
```



## 次のステップ

- vCloud Director Web Console にアクセスするには、`https://hostname.domain.tld/cloud` に移動し、システム管理者としてログインするか、`https://vcloud.example.com/cloud/org/myOrg` にログインして組織にログインします。vCloud Director Web Console の詳細については、vCloud Director 管理者ガイド バージョン 9.7 および vCloud Director ユーザー ガイド バージョン 9.7 を参照してください。
- vCloud Director Web Console を無効にしてデフォルトの動作に戻すには、次のコマンドを実行します。

```
cell-management-tool manage-config -n flex.ui.enabled -v false
```

## レガシー API エンドポイントへのサービス プロバイダ アクセスの無効化

vCloud Director 10.0 以降では、サービス プロバイダおよびテナントから vCloud Director へのアクセスに、個別の vCloud Director OpenAPI ログイン エンドポイントを使用できます。

vCloud Director 10.0 では、vCloud Director へのアクセスを制限することによってセキュリティを強化できる、新しい OpenAPI エンドポイントが 2 つ導入されています。

- `/cloudapi/1.0.0/sessions/provider`: サービス プロバイダ ログイン用の OpenAPI エンドポイント。テナントは、このエンドポイントを使用して vCloud Director にアクセスすることはできません。
- `/cloudapi/1.0.0/sessions/` - テナント ログイン用の OpenAPI エンドポイント。サービス プロバイダは、このエンドポイントを使用して vCloud Director にアクセスすることはできません。

デフォルトでは、プロバイダ管理者および組織のユーザーが vCloud Director にアクセスするには、`/api/sessions` API エンドポイントにログインします。

セル管理ツールの `manage-config` サブコマンドを使用すると、サービス プロバイダから `/api/sessions` API エンドポイントへのアクセスを無効にできるため、プロバイダのログインを、サービス プロバイダのみがアクセスできる新しい `/cloudapi/1.0.0/sessions/provider` OpenAPI エンドポイントに制限することができます。

## 手順

- 1 いずれかの vCloud Director セルの OS に、**root** としてログインするか、SSH で接続します。
- 2 プロバイダから `/api/sessions` API エンドポイントへのアクセスをブロックするには、セル管理ツールを使用して、次のコマンドを実行します。

```
/opt/vmware/vcloud-director/bin/cell-management-tool manage-config -n  
vcloud.api.legacy.nonprovideronly -v true
```

## 結果

これで、サービス プロバイダから `/api/sessions` API エンドポイントにアクセスできなくなります。サービス プロバイダは、新しい OpenAPI エンドポイント `/cloudapi/1.0.0/sessions/provider` を使用して vCloud Director にアクセスできます。テナントは、`/api/sessions` API エンドポイントと新しい `/cloudapi/1.0.0/sessions/` OpenAPI エンドポイントの両方を使用して、vCloud Director にアクセスできます。

## 次のステップ

プロバイダから /api/sessions API エンドポイントにアクセスできるようにするには、次のコマンドを実行します。

```
/opt/vmware/vcloud-director/bin/cell-management-tool manage-config -n
vcloud.api.legacy.nonprovideronly -v false
```

## セルの管理

セル管理ツールの cell サブコマンドを使用すると、タスク スケジューラをサスペンドして新しいタスクを開始できないようにしたり、アクティブなタスクのステータスを表示したり、セルのメンテナンス モードをコントロールしたり、セルを正常にシャットダウンしたりすることができます。

セルを管理するには、次の形式でコマンドラインを使用します。

```
cell-management-tool cell -u sysadmin-username -p sysadmin-password option
```

ここで、*sysadmin-username* および *sysadmin-password* は、システム管理者のユーザー名およびパスワードです。

**注：** セキュリティ上の理由により、パスワードは省略できます。この場合、パスワードは画面に表示されず、パスワードの入力を求めるプロンプトが表示されます。

システム管理者の認証情報を入力する代わりに、--pid オプションを使用して、セル プロセスのプロセス ID を入力することもできます。セルのプロセス ID を検索するには、次のようなコマンドを使用します。

```
cat /var/run/vmware-vcd-cell.pid
```

表 10-3. セル管理ツールのオプションと引数、cell サブコマンド

オプション	引数	説明
--help (-h)	なし	このカテゴリで使用可能なコマンドの概要を示します。
--pid (-i)	セル プロセスのプロセス ID	このオプションは -username の代わりに使用できます。
--maintenance (-m)	true または false	セルをメンテナンス モードに設定します。  引数 true を指定すると、セルのアクティビティは静止し、セルがメンテナンス モードになります。  引数 false により、セルのメンテナンス モードが解除されます。
--password (-p)	vCloud Director システム管理者のパスワード	-username オプションが使用されている場合は、オプションです。  このオプションを省略した場合、パスワードは画面に表示されず、パスワードの入力を求めるプロンプトが表示されます。

表 10-3. セル管理ツールのオプションと引数、cell サブコマンド（続き）

オプション	引数	説明
--quiesce (-q)	true または false	セル上のアクティビティを静止します。 引数 true はスケジューラを中断します。 引数 false はスケジューラを再開します。
--shutdown (-s)	なし	サーバ上の vCloud Director サービスを正常にシャットダウンします。
--status (-t)	なし	セル上で実行されているタスクの数とセルのステータスに関する情報を表示します。
--status-verbose (-tt)	なし	セル上で実行されているタスクとセルのステータスに関する詳細情報を表示します。
--username (-u)	vCloud Director システム管理者 のユーザー名	このオプションは -pid の代わりに使用できます。

## セル アプリケーションの管理

セルの起動時に実行される一連のアプリケーションを管理するには、セル管理ツールの cell-application コマンドを使用します。

vCloud Director は vCloud Director クライアントが必要とするサービスを提供するさまざまなアプリケーションを実行します。セルはこれらのアプリケーションのサブセットをデフォルトで実行します。通常、vCloud Director のインストールをサポートするには、このサブセットに含まれるすべてのアプリケーションが必要になります。

セルの起動時に実行されるアプリケーションのリストを表示または変更するには、次の形式のコマンドラインを使用します。

```
cell-management-tool -u sysadmin-username -p sysadmin-password cell-application command
```

### ***sysadmin-username***

vCloud Director システム管理者のユーザー名。

### ***sysadmin-password***

vCloud Director システム管理者のパスワード。パスワードに特殊文字が含まれている場合はパスワードを引用符で囲む必要があります。

**注：** `cell-management-tool` コマンド ラインに vCloud Director システム管理者のパスワードを入力することもできますが、パスワードを省略するほうが安全です。これにより、`cell-management-tool` でパスワードが要求されるようになりますが、入力内容は画面には表示されません。

システム管理者の認証情報を入力する代わりに、`--pid` オプションを使用して、セル プロセスのプロセス ID を入力することもできます。セルのプロセス ID を検索するには、次のようなコマンドを使用します。

```
cat /var/run/vmware-vcd-cell.pid
```

## command

`cell-application` サブコマンド。

表 10-4. セル管理ツールのオプションと引数、`cell-application` サブコマンド

コマンド	引数	説明
<code>--help (-h)</code>	なし	このカテゴリで使用可能なコマンドの概要を示します。
<code>--application-states</code>	なし	セル アプリケーションと各アプリケーションの現在の状態を一覧表示します。
<code>--disable</code>	アプリケーション ID	セルの起動時にこのセル アプリケーションが実行されないようになります。
<code>--enable</code>	アプリケーション ID	セルの起動時にこのセル アプリケーションが実行されるようになります。
<code>--pid (-i)</code>	セル プロセスのプロセス ID	このオプションは <code>-u</code> または <code>-u</code> および <code>-p</code> の代わりに使用できます。
<code>--list</code>	なし	すべてのセル アプリケーションを一覧表示し、セルの起動時に実行するように設定されているかどうかを示します。
<code>--password (-p)</code>	vCloud Director 管理者パスワード	任意。コマンドラインでパスワードが入力されていない場合、コマンドの実行時にパスワードの入力を求めるプロンプトが表示されます。
<code>--set</code>	セミコロンで区切られたアプリケーション ID のリスト。	セルの起動時に実行するセル アプリケーションのセットを指定します。次のコマンドを使用すると、セルの起動時に起動するように設定されたセル アプリケーションの既存のセットが上書きされます。1 つのアプリケーションの起動状態を変更するには、 <code>--enable</code> または <code>--disable</code> を使用します。
<code>--username (-u)</code>	vCloud Director 管理者ユーザー名。	<code>--pid</code> を指定しない場合は必須

## 例：セル アプリケーションとその起動状態の一覧表示

次の `cell-management-tool` コマンドラインを実行すると、セル アプリケーションとその起動状態のリストが返されます。コマンドの実行にはシステム管理者の認証情報が必要です。

```
[root@cell1 /opt/vmware/vcloud-director/
bin]# ./cell-management-tool -u administrator cell-application --list
Please enter the administrator password:
```

```
name                id                enabled  description
```

Networking	com.vmware.vc... true	Exposes NSX api endpoints directly from vCD.
Console Proxy	com.vmware.vc... true	Proxies VM console data connection...
Cloud Proxy	com.vmware.vc... true	Proxies TCP connections from a tenant site.
Compute Service Broker	com.vmware.vc... true	Allows registering with a service control...
Maintenance Application	com.vmware.vc... false	Indicates to users the cell is undergo ...
Core Cell Application	com.vmware.vc... true	Main cell application, Flex UI and REST API.

## データベース接続プロパティを更新する

セル管理ツールの `reconfigure-database` サブコマンドを使用すると、vCloud Director データベースの接続プロパティを更新できます。

vCloud Director のインストール プロセスまたは vCloud Director アプライアンスのデプロイ プロセスで、データベース タイプとデータベース接続のプロパティを設定します。[5 章 Linux への vCloud Director のインストール](#)および[6 章 vCloud Director アプライアンスのデプロイ](#)を参照してください。

vCloud Director データベースを設定した後に、`reconfigure-database` サブコマンドを使用してデータベース接続を更新できます。既存の vCloud Director データベースの新しいホストへの移動、データベースのユーザー名またはパスワードの変更、PostgreSQL データベースの SSL 接続の有効化を行うことができます。

```
cell-management-tool reconfigure-database options
```

**重要：** `reconfigure-database` コマンドを実行して加えられた変更は、セルのグローバル構成ファイル `global.properties` および応答ファイル `responses.properties` に書き込まれます。コマンドを実行する前に、応答ファイルが `/opt/vmware/vcloud-director/etc/responses.properties` にあり、書き込み可能であることを確認してください。応答ファイルの保護と再利用の詳細については、「[5 章 Linux への vCloud Director のインストール](#)」を参照してください。

`--pid` オプションを使用しない場合は、セルを再起動して変更を適用する必要があります。

表 10-5. セル管理ツールのオプションと引数、`reconfigure-database` サブコマンド

オプション	引数	説明
<code>--help</code> ( <code>-h</code> )	なし	このカテゴリで使用可能なオプションの概要を示します。
<code>--database-host</code> ( <code>-dbhost</code> )	vCloud Director データベース ホストの IP アドレスまたは完全修飾ドメイン名	<code>database.jdbcUrl</code> プロパティの値を更新します。 <b>重要：</b> このコマンドは、値の形式のみを検証します。
<code>--database-instance</code> ( <code>-dbinstance</code> )	SQL Server データベース インスタンス	オプション。データベース タイプが <code>sqlserver</code> の場合に使用します。 <b>重要：</b> このオプションを指定する場合は、最初にデータベースを設定したときと同じ値を指定する必要があります。
<code>--database-name</code> ( <code>-dbname</code> )	データベース サービス名。	<code>database.jdbcUrl</code> プロパティの値を更新します。

表 10-5. セル管理ツールのオプションと引数、reconfigure-database サブコマンド（続き）

オプション	引数	説明
<code>--database-password</code> ( <code>-dbpassword</code> )	データベース ユーザーのパスワード。	<code>database.password</code> プロパティの値を更新します。指定したパスワードは暗号化されてからプロパティ値として格納されます。
<code>--database-port</code> ( <code>-dbport</code> )	データベース ホスト上で動作するデータベース サービスによって使用されるポート番号。	<code>database.jdbcUrl</code> プロパティの値を更新します。  <b>重要：</b> このコマンドは、値の形式のみを検証します。
<code>--database-type</code> ( <code>-dbtype</code> )	データベース タイプ。次のいずれか： ■ <code>sqlserver</code> ■ <code>postgres</code>	<code>database.jdbcUrl</code> プロパティの値を更新します。
<code>--database-user</code> ( <code>-dbuser</code> )	データベース ユーザーのユーザー名	<code>database.user</code> プロパティの値を更新します。
<code>--database-ssl</code>	<code>true</code> または <code>false</code>	データベース タイプが <code>postgres</code> の場合に使用します。vCloud Director からの SSL 接続を要求するように、PostgreSQL データベースを設定します。
<code>--pid</code> ( <code>-i</code> )	セルのプロセス ID。	オプション。実行中の vCloud Director セルにホット再構成を実行します。セルを再起動する必要はありません。  <code>--private-key-path</code> と一緒に使用した場合は、ローカルおよびリモートのセルにコマンドを直ちに実行できます。
<code>--private-key-path</code>	セルのプライベート キーへのパス名。	オプション。サーバ グループ内のすべてのセルが正常にシャットダウンされ、そのデータベース プロパティが更新され、再起動されます。  <b>重要：</b> すべてのセルは、パスワードを要求せずにスーパー ユーザーからの SSH 接続を許可する必要があります。
<code>--remote-sudo-user</code>	<code>sudo</code> 権限を持つユーザーの名前。	リモート ユーザーが <code>root</code> と異なる場合に、 <code>--private-key-path</code> オプションと一緒に使用します。  アプライアンスの場合は、 <code>postgres</code> ユーザーにこのオプションを使用できます ( <code>--remote-sudo-user=postgres</code> など)。

オプション `--database-host` および `--database-port` を使用した場合、コマンドでは引数の形式は検証されますが、ホストとポートの組み合わせでネットワークにアクセスできるかどうか、または指定したタイプで実行中のデータベースがあるかどうかは確認されません。

--private-key-path オプションを使用する場合、パスワードを要求せずにスーパー ユーザーからの SSH 接続を許可するように、すべてのセルを構成する必要があります。たとえば、検証を実行するには、次の Linux コマンドを実行します。

```
sudo -u vcloud ssh -i private-key-path root@cell-ip
```

この例では、ID が vcloud に設定され、*cell-ip* にあるセルへの SSH 接続が root として確立されますが、root パスワードの指定はありません。ローカル セルの *private-key-path* にあるプライベート キーがユーザー vcloud.vcloud から読み取り可能で、対応するパブリック キーが *cell-ip* の root ユーザーの *authorized-keys* ファイルにあれば、コマンドが成功します。

**注：** vCloud Director プロセスを実行する ID として使用するため、vCloud Director インストーラにより、vcloud ユーザー、vcloud グループ、および vcloud.vcloud アカウントが作成されます。vcloud ユーザーにはパスワードがありません。

## 例： vCloud Director データベースのユーザー名とパスワードを変更する

vCloud Director データベースのユーザー名とパスワードを変更し、他のすべての接続プロパティを最初に設定したままにしておくには、次のコマンドを実行します。

```
[root@cell1 /opt/vmware/vcloud-director/  
bin]#cell-management-tool reconfigure-database \ -dbuser vcd-dba -dbpassword P@55w@rd
```

## 例： すべてのセルのホット再構成による vCloud Director データベースの IP アドレスの更新

sudo 権限を持つ非 root ユーザーがすべてのセルの vCloud Director データベースの IP アドレスを直ちに変更するには、次のコマンドを実行します。

```
[sudo@cell1 /opt/vmware/vcloud-director/  
bin]#cell-management-tool reconfigure-database \ --dbhost db_ip_address -i $(service vmware-vcd pid  
cell) --private-key-path=path_to_private-key \ --remote-sudo-user=non-root-user
```

## 破損したスケジューラ データの検出および修復

vCloud Director は、クォーツ ジョブ スケジューラを使用して、システムで実行されている非同期操作（ジョブ）を連携します。クォーツ スケジューラ データベースが破損すると、システムを正常に静止できない場合があります。スケジューラ データの破損の有無を確認するには、セル管理ツールの *fix-scheduler-data* コマンドを使用して、データベースをスキャンします。データが破損していた場合は、必要に応じて修復します。

データベース内で破損したスケジューラ データをスキャンするには、次の形式のコマンド ラインを使用します。

```
cell-management-toolfix-scheduler-dataoptions
```

表 10-6. セル管理ツールのオプションと引数、fix-scheduler-data サブコマンド

オプション	引数	説明
--help (-h)	なし	このカテゴリで使用可能なコマンドの概要を示します。
--dbuser	vCloud Director データベース ユーザーのユーザー名。	コマンドラインで指定する必要があります。
--dbpassword	vCloud Director データベース ユーザーのパスワード。	指定しない場合に入力が求められます。

## HTTP およびコンソール プロキシ エンドポイントの自己署名証明書の生成

セル管理ツールの `generate-certs` コマンドを使用して、HTTP およびコンソール プロキシ エンドポイントの自己署名付き SSL 証明書を生成します。

各 vCloud Director サーバ グループは 2 台の SSL エンドポイントをサポートする必要があります。1 台は HTTP サービスのエンドポイント、もう 1 台はコンソール プロキシ サービスのエンドポイントです。HTTP サービスのエンドポイントでは、vCloud Director Service Provider Admin Portal、vCloud Director Tenant Portal、および vCloud API をサポートします。リモート コンソール プロキシのエンドポイントでは、vApp および仮想マシンへの VMRC 接続をサポートします。

セル管理ツールの `generate-certs` コマンドにより、[Linux 上での vCloud Director 用の自己署名付き SSL 証明書の作成](#)に示す手順が自動化されます。

新しい自己署名付き SSL 証明書を生成して新規または既存のキーストアに追加するには、次の形式でコマンドラインを使用します。

```
cell-management-tool generate-certs options
```

表 10-7. セル管理ツールのオプションと引数、generate-certs サブコマンド

オプション	引数	説明
--help (-h)	なし	このカテゴリで使用可能なコマンドの概要を示します。
--expiration (-x)	<i>days-until-expiration</i>	証明書の有効期限が切れるまでの日数です。デフォルトでは 365 です。
--issuer (-i)	<i>name=value [, name=value, ...]</i>	証明書発行者の X.509 識別名。デフォルトでは CN= <i>FQDN</i> です。 <i>FQDN</i> はセルの完全修飾ドメイン名です。完全修飾ドメイン名が使用できない場合は、その IP アドレスです。複数の属性と値のペアを指定する場合は、各ペアをカンマで区切り、引数全体を引用符で囲んでください。
--httpcert (-j)	なし	HTTP エンドポイントの証明書を生成します。



表 10-7. セル管理ツールのオプションと引数、generate-certs サブコマンド（続き）

オプション	引数	説明
--key-size (-s)	<i>key-size</i>	整数ビットとして表されるキー ペアのサイズです。デフォルトでは 2048 です。NIST Special Publication 800-131A に従い、1,024 未満のキー サイズはサポートされなくなりました。
--keystore-pwd (-w)	<i>keystore-password</i>	このホスト上のキーストアのパスワードです。
--out (-o)	<i>keystore-pathname</i>	このホスト上のキーストアへのフル パス名です。
--consoleproxycert (-p)	なし	コンソール プロキシ エンドポイントの証明書を作成します。

**注：** このサブコマンドの以前のリリースとの互換性を維持するために、`-j` と `-p` の両方を省略すると、`-j` と `-p` を両方指定した場合と同じ結果となります。

## 例： 自己署名付き証明書の作成

これらの両方の例では、キーストアが `/tmp/cell.ks` に存在し、パスワードが `kspw`であることを想定しています。このキーストアは、まだ存在しない場合には作成されます。

この例では、デフォルト値を使用して新しい証明書を作成します。発行者名は `CN=Unknown` に設定されています。証明書はキー長にデフォルトの 2048 ビットを使用し、作成後 1 年で期限切れになります。

```
[root@cell1 /opt/vmware/vcloud-director/
bin]# ./cell-management-tool generate-certs -j -p -o /tmp/cell.ks -w kspw
New keystore created and written to /tmp/cell.ks.
```

この例では HTTP エンドポイント専用の新しい証明書を作成します。また、キー サイズおよび発行者名を示すカスタム値を指定します。発行者名は `CN=Test`, `L=London`, `C=GB` に設定されています。HTTP 接続の新しい証明書のキー長は 4,096 ビットで、作成後 90 日で期限が切れます。コンソール プロキシ エンドポイントの既存の証明書は影響を受けません。

```
[root@cell1 /opt/vmware/vcloud-director/
bin]# ./cell-management-tool generate-certs -j -o /tmp/cell.ks -w kspw -i "CN=Test, L=London, C=GB"
-s 4096 -x 90
New keystore created and written to /tmp/cell.ks.
```

**重要：** キーストア ファイルおよびキーストア ファイルが格納されているディレクトリは、ユーザー `vcloud.vcloud` から読み取り可能である必要があります。vCloud Director インストーラにより、このユーザーとグループが作成されます。

## HTTP およびコンソール プロキシ エンドポイントの証明書の置き換え

セル管理ツールの `certificates` コマンドを使用して、HTTP およびコンソール プロキシ エンドポイントの SSL 証明書を置き換えます。

セル管理ツールの `certificates` コマンドにより、JCEKS キーストアに保存されている新しい証明書で既存の証明書を置き換えるプロセスが自動化されます。`certificates` コマンドを使用して、自己署名証明書を署名付き証明書に、または有効期限が切れる証明書を新しい証明書を置き換えます。署名付き証明書を保存する JCEKS キーストアを作成するには、[Linux 上での vCloud Director 用の自己署名付き SSL 証明書の作成](#)を参照してください。

エンドポイントのいずれかまたは両方の SSL 証明書を置き換えるには、次の形式でコマンドを使用します。

```
cell-management-tool certificates options
```

表 10-8. セル管理ツールのオプションと引数、`certificates` サブコマンド

オプション	引数	説明
<code>--help (-h)</code>	なし	このカテゴリで使用可能なコマンドの概要を示します。
<code>--config (-c)</code>	セルの <code>global.properties</code> ファイルへのフル パス名	デフォルト値は、 <code>\$VCLLOUD_HOME/etc/global.properties</code> です。
<code>--httpks (-j)</code>	なし	http エンドポイントによって使用される <code>certificates</code> という名前のキーストア ファイルを置換します。
<code>--consoleproxyks (-p)</code>	なし	コンソール プロキシ エンドポイントによって使用される <code>proxycertificates</code> という名前のキーストア ファイルを置換します。
<code>--responses (-r)</code>	セルの <code>responses.properties</code> ファイルへのフル パス名	デフォルトで <code>\$VCLLOUD_HOME/etc/responses.properties</code> です。
<code>--keystore (-k)</code>	<i>keystore-pathname</i>	署名付き証明書が保存されている JCEKS キーストアへのフル パス名です。 <code>-k</code> に置き換えられる非推奨の <code>-s</code> 短縮形
<code>--keystore-password (-w)</code>	<i>keystore-password</i>	<code>--keystore</code> オプションによって参照される JCEKS キーストアのパスワードです。非推奨の <code>-kspassword</code> および <code>--keystorepwd</code> オプションを置き換えます。

## 例： 証明書の置換

--config オプションと --responses オプションは、そのデフォルトの場所から移動されていない限り、省略できます。この例では、キーストアが /tmp/my-new-certs.ks に存在し、パスワードは kspw となっています。この例では、セルの既存の HTTP エンドポイント証明書を /tmp/my-new-certs.ks 内の証明書で置き換えます。

```
[root@cell1 /opt/vmware/vcloud-director/
bin]# ./cell-management-tool certificates -j -k /tmp/my-new-certs.ks -w kspw
Certificate replaced by user specified keystore at /tmp/new.ks.
You will need to restart the cell for changes to take effect.
```

**注：** 証明書を置換した後は、セルを再起動する必要があります。

## 外部サービスからの SSL 証明書のインポート

セル管理ツールの import-trusted-certificates コマンドを使用して、AMQP や vCloud Director データベースなどの外部サービスへのセキュアな接続の確立に使用する証明書をインポートします。

外部サービスへのセキュアな接続を作成するには、vCloud Director で、外部サービスの証明書を固有のトラストストアにインポートして、そのサービスの有効な信頼チェーンを確立する必要があります。信頼されている証明書をセルのトラストストアにインポートするには、次の形式でコマンドを使用します。

```
cell-management-tool import-trusted-certificates options
```

表 10-9. セル管理ツールのオプションと引数、import-trusted-certificates サブコマンド

オプション	引数	説明
--help(-h)	なし	このカテゴリで使用可能なコマンドの概要を示します。
--destination	パス名	ターゲットのトラストストアへのフル パス名。コマンドラインで指定されていない場合は、デフォルトで /opt/vmware/vcloud-director/etc/certificates が使用されます。
--destination-password	文字列	ターゲットのトラストストアのパスワード。コマンドラインで指定されていない場合、デフォルトは vcloud.ssl.truststore.password の値で設定されます。
--destination-type	キーストアのタイプ	ターゲットのトラストストアのキーストア タイプ。JKS または JCEKS のいずれかにできます。デフォルトでは JCEKS です。
--force	なし	ターゲットのトラストストア内の既存の証明書を上書きします。
--source	パス名	ソース PEM ファイルへのフル パス名。

## 例：信頼されている証明書のインポート

この例では、証明書を「/tmp/demo.pem」から「/opt/vmware/vcloud-director/etc/certificates」の vCloud Director ローカル キーストアにインポートします。vCloud Director はキーストアのパスワードを `import-trusted-certificates` コマンドで復号される暗号化形式で格納します。

```
[root@cell1 /opt/vmware/vcloud-director/
bin]# ./cell-management-tool import-trusted-certificates --source /tmp/demo.pem
```

## 許可された SSL 暗号のリストの管理

SSL ハンドシェイク プロセス中に使用するためにセルが提供する暗号化スイートのセットを構成するには、セル管理ツールの `ciphers` コマンドを使用します。

クライアントが vCloud Director セルとの SSL 接続を確立すると、セルはデフォルトの許可暗号リスト上で構成された暗号のみを使用するよう提案します。接続を保護する十分な強度がないか、あるいは SSL 接続障害の原因となることがわかっているために、このリストに含まれていない暗号があります。vCloud Director をインストールまたはアップグレードすると、インストールまたはアップグレードのスクリプトがセルの証明書を調べます。いずれかの証明書が許可暗号リストに含まれていない暗号を使用して暗号化されている場合、スクリプトはセルの構成を変更してこの暗号の使用を許可し、警告を表示します。これらの暗号を利用しながら既存の証明書を引き続き使用することも、次の手順を実行して証明書を置き換え、許可暗号リストを再構成することもできます。

- 1 禁止されたとの暗号も使用しない新しい証明書を作成します。[許可されているすべての暗号の一覧表示](#)に示された `cell-management-tool ciphers -a` を使用して、デフォルト構成で許可されている暗号をすべて一覧表示することができます。
- 2 `cell-management-tool certificates` コマンドを使用すると、セルの既存の証明書が新しい証明書で置き換えられます。
- 3 `cell-management-tool ciphers` コマンドを使用すると、許可暗号リストを再構成して、新しい証明書で使用されない暗号を除外することができます。これらの暗号を除外すると、ハンドシェイク中に提供される暗号数が実用的な最小数まで減るため、セルとの SSL 接続を確立するまでの時間が短縮されます。

**重要：** VMRC コンソールでは AES256-SHA および AES128-SHA 暗号を使用する必要があるため、vCloud Director クライアントで VMRC コンソールを使用する場合は、これらを禁止できません。

許可されている SSL 暗号のリストを管理するには、次の形式のコマンド ラインを使用します。

```
cell-management-tool ciphers options
```

表 10-10. セル管理ツールのオプションと引数、`ciphers` サブコマンド

オプション	引数	説明
<code>--help (-h)</code>	なし	このカテゴリで使用可能なコマンドの概要を示します。
<code>--all-allowed (-a)</code>	なし	許可されているすべての暗号を一覧表示します。

表 10-10. セル管理ツールのオプションと引数、ciphers サブコマンド（続き）

オプション	引数	説明
<code>--compatible-reset (-c)</code>	なし	デフォルトの許可暗号リストにリセットし、さらにこのセルの証明書で使用する暗号を許可します。
<code>--disallow (-d)</code>	<a href="https://www.openssl.org/docs/man1.0.2/man1/ciphers.html">https://www.openssl.org/docs/man1.0.2/man1/ciphers.html</a> で公開されている、暗号名のカンマ区切りリスト	指定されたカンマ区切りリストで暗号を禁止します。
<code>--list (-l)</code>	なし	現在構成されている暗号を一覧表示します。
<code>--reset (-r)</code>	なし	デフォルトの許可暗号リストにリセットします。このセルの証明書で禁止された暗号が使用されている場合は、許可された暗号を使用する新しい証明書をインストールするまで、このセルとの SSL 接続は確立できません。

## 例：許可されているすべての暗号の一覧表示

`--all-allowed (-a)` オプションを使用すると、このセルが SSL ハンドシェイク中に提供することが許可されている暗号がすべて一覧表示されます。

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./cell-management-tool ciphers -a
* TLS_DHE_DSS_WITH_AES_256_CBC_SHA
* TLS_DHE_DSS_WITH_AES_128_CBC_SHA
* TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA
* TLS_DHE_RSA_WITH_AES_256_CBC_SHA
* TLS_DHE_RSA_WITH_AES_128_CBC_SHA
* TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
* TLS_RSA_WITH_AES_256_CBC_SHA
* TLS_RSA_WITH_AES_128_CBC_SHA
* TLS_RSA_WITH_3DES_EDE_CBC_SHA
* TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
* TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
* TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA
* TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
* TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
* TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
* TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA
* TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA
* TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA
* TLS_ECDH_RSA_WITH_AES_256_CBC_SHA
* TLS_ECDH_RSA_WITH_AES_128_CBC_SHA
* TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA
* SSL_RSA_WITH_3DES_EDE_CBC_SHA
* SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA
```

## 例：2つの暗号の禁止

許可暗号リストから1つ以上の暗号を削除するには、`--disallow (-d)` オプションを使用します。このオプションには1つ以上の暗号名を指定する必要があります。カンマ区切りリストでは、複数の暗号名を指定できます。`ciphers -a` の出力からこのリストの名前を取得できます。次の例では、前の例で一覧表示された2つの暗号を削除します。

```
[root@cell1 /opt/vmware/vcloud-director/
bin]# ./cell-management-tool ciphers -d
SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA,SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA
```

## 許可された SSL プロトコルのリストの管理

SSL ハンドシェイク プロセス中にセルが使用を提案する SSL プロトコルのセットを構成するには、セル管理ツールの `ssl-protocols` コマンドを使用します。

クライアントが vCloud Director セルとの SSL 接続を確立すると、セルは許可された SSL プロトコルのリスト上で構成されたプロトコルのみを使用するよう提案します。TLSv1、SSLv3、SSLv2Hello などのプロトコルには重大なセキュリティ上の脆弱性があることがわかっているため、デフォルトのリストには含まれていません。

許可されている SSL プロトコルのリストを管理するには、次の形式のコマンド ラインを使用します。

```
cell-management-tool ssl-protocols options
```

表 10-11. セル管理ツールのオプションと引数、`ssl-protocols` サブコマンド

オプション	引数	説明
<code>--help (-h)</code>	なし	このカテゴリで使用可能なコマンドの概要を示します。
<code>--all-allowed (-a)</code>	なし	vCloud Director がサポートできるすべての SSL プロトコルをリストします。
<code>--disallow (-d)</code>	SSL プロトコル名のカンマ区切りのリスト	許可されない SSL プロトコルのリストを、リスト内で指定されたプロトコルに再構成します。
<code>--list (-l)</code>	なし	vCloud Director が現在サポートするように構成されている、許可された SSL プロトコルのセットをリストします。
<code>--reset (-r)</code>	なし	構成された SSL プロトコルのリストを出荷時のデフォルトにリセットします。

**重要：** `ssl-protocols --disallow` または `ssl-protocols reset` を実行した後は、セルを再起動する必要があります。

## 例：許可され構成された SSL プロトコルの一覧表示

--all-allowed (-a) オプションを使用すると、このセルが SSL ハンドシェイク中に提供することが許可されている SSL プロトコルがすべて一覧表示されます。

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./cell-management-tool ssl-protocols -a
Product default SSL protocols:

* TLSv1.2
* TLSv1.1
* TLSv1
* SSLv3
* SSLv2Hello
```

このリストは通常、セルがサポートするように構成された SSL プロトコルのスーパーセットです。これらの SSL プロトコルを一覧表示するには、--list (-l) オプションを使用します。

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./cell-management-tool ssl-protocols -l
Allowed SSL protocols:

* TLSv1.2
* TLSv1.1
```

## 例：許可されない SSL プロトコルのリストの再構成

--disallow (-d) オプションを使用すると、許可されない SSL プロトコルのリストが再構成されます。このオプションを使用するには、ssl-protocols -a によって生成された許可されるプロトコルのサブセットのコンマ区切りのリストが必要です。

この例では、許可される SSL プロトコルのリストを更新し、TLSv1 が含まれるようにしています。5.5 Update 3e より前の VMware® vCenter™ リリースには TLSv1 が必要です。

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./cell-management-tool ssl-protocols -d SSLv3,SSLv2Hello
```

このコマンドを実行した後は、セルを再起動する必要があります。

## メトリック収集の設定

セル管理ツールの configure-metrics コマンドを使用して、収集するメトリックのセットを設定します。

vCloud Director は、仮想マシンのパフォーマンスおよびリソース消費に関する現在および過去の情報を提供するメトリックを収集できます。このサブコマンドを使用して、vCloud Director によって収集されるメトリックを設定します。cell-management-tool cassandra サブコマンドを使用して、vCloud Director メトリック リポジトリとして使用するための Apache Cassandra データベースを設定します。[Cassandra メトリック データベースの構成](#) を参照してください。

vCloud Director によって収集されるメトリックを設定するには、次の形式でコマンド ラインを使用します。

```
cell-management-tool configure-metrics --metrics-config pathname
```

表 10-12. セル管理ツールのオプションと引数、configure-metrics サブコマンド

コマンド	引数	説明
--help (-h)	なし	このカテゴリで使用可能なコマンドの概要を示します。
--repository-host (廃止されました)	KairosDB ホストのホスト名または IP アドレス	廃止されました。cell-management-tool cassandra サブコマンドの --cluster-nodes オプションを使用して、vCloud Director メトリック リポジトリとして使用するための Apache Cassandra データベースを設定します。
--repository-port (廃止されました)	使用する KairosDB ポート。	廃止されました。cell-management-tool cassandra サブコマンドの --port オプションを使用して、vCloud Director メトリック リポジトリとして使用するための Apache Cassandra データベースを設定します。
--metrics-config	パス名	メトリック設定ファイルへのパス

## 例：メトリック データベース接続の構成

この例では、/tmp/metrics.groovy ファイルで指定されているように、メトリック収集を設定します。

```
[root@cell1 /opt/vmware/vcloud-director/
bin]# ./cell-management-tool configure-metrics --metrics-config /tmp/metrics.groovy
```

vCloud Director メトリック収集サービスでは、vSphere Performance Manager で収集されたメトリックのサブセットを実装します。メトリック名と収集パラメータの詳細については、vSphere Performance Manager のドキュメントを参照してください。metrics-config ファイルでは、1 つ以上のメトリック名を列挙し、列挙した各メトリックの収集パラメータを提供します。以下にその例を挙げます。

```
configuration {
    metric("cpu.usage.average")
    metric("cpu.usagemhz.average")
    metric("cpu.usage.maximum")
    metric("disk.used.latest") {
        currentInterval=300
        historicInterval=300
        entity="VM"
        instance=""
        minReportingInterval=1800
        aggregator="AVERAGE"
    }
}
```

次のメトリック名がサポートされています。



表 10-13. メトリック名

メトリック名	説明
cpu.usage.average	この仮想マシンでアクティブに使用される平均 CPU（使用可能な合計 CPU を占める割合）のホストのビュー。すべてのソケットのすべてのコアが含まれます。
cpu.usagemhz.average	この仮想マシンでアクティブに使用される平均 CPU（実際の測定値）のホストのビュー。すべてのソケットのすべてのコアが含まれます。
cpu.usage.maximum	この仮想マシンでアクティブに使用される最大 CPU（使用可能な合計 CPU を占める割合）のホストのビュー。すべてのソケットのすべてのコアが含まれます。
mem.usage.average	この仮想マシンによって使用されるメモリ（構成済みの合計メモリを占める割合）。
disk.provisioned.latest	含まれる組織仮想データセンターで、この仮想ハード ディスクに割り当てられたストレージ容量。
disk.used.latest	すべての仮想ハード ディスクによって使用されるストレージ。
disk.read.average	すべての仮想ハード ディスクの平均読み取り比率。
disk.write.average	すべての仮想ハード ディスクの平均書き込み比率。

**注：** 仮想マシンに複数のディスクが含まれる場合、メトリックはすべてのディスクの集計として報告されます。CPU メトリックは、すべてのコアおよびソケットの集計です。

名前付きの各メトリックについては、次の収集パラメータを指定できます。

表 10-14. メトリック収集パラメータ

パラメータ名	値	説明
currentInterval	秒を示す整数。	現在のメトリックのクエリで、最新の使用可能なメトリック値のクエリ時に使用する間隔（秒）。指定しない場合は、デフォルトで 20 が使用されます。20 を超える値がサポートされるのは、vSphere Performance Manager で定義されている、レベル 1 のメトリックに対してのみです。
historicInterval	秒を示す整数。	履歴のメトリック値のクエリ時に使用する間隔（秒）です。指定しない場合は、デフォルトで 20 が使用されます。20 を超える値がサポートされるのは、vSphere Performance Manager で定義されている、レベル 1 のメトリックに対してのみです。
entity	HOST、VM のいずれか	メトリックを使用できる vCenter Server オブジェクトのタイプ。指定しない場合は、デフォルトで VM が使用されます。エンティティによっては、使用できないメトリックもあります。
instance	vSphere Performance Manager の PerfMetricId インスタンス識別子。	メトリックの個々のインスタンス（たとえば、個々の CPU コア）、すべてのインスタンスの集計、またはその両方のデータを取得するかを指定します。 "*" の値を指定すると、すべてのメトリック、インスタンス、および集計のデータが収集されます。空の文字列 "" を指定すると、集計データのみが収集されます。"DISKFILE" のような固有の文字列では、そのインスタンスのみのデータが収集されます。省略した場合のデフォルト値は、 "*" です。

表 10-14. メトリック収集パラメータ（続き）

パラメータ名	値	説明
minReportingInterval	秒を示す整数。	時系列データのレポートに使用する、デフォルトの集計間隔（秒）を指定します。収集間隔の頻度が不十分である場合に、レポートの頻度を調整できます。デフォルトは 0 です（レポート用の間隔は指定しない）。
aggregator	AVERAGE、MINIMUM、MAXIMUM、SUMMATION のいずれか	minReportingInterval の間に実行される集計のタイプです。省略した場合のデフォルト値は、AVERAGE です。

## Cassandra メトリック データベースの構成

セルをオプションのメトリック データベースに接続するには、セル管理ツールの `cassandra` コマンドを使用します。

vCloud Director は、仮想マシンのパフォーマンスおよびリソース消費に関する現在および過去の情報を提供するメトリックを収集できます。このサブコマンドを使用して、vCloud Director メトリック リポジトリとして使用するための Apache Cassandra データベースを設定します。 `cell-management-tool configure-metrics` サブコマンドを使用して、収集するメトリックのセットを設定します。 [メトリック収集の設定](#)を参照してください。

履歴メトリックのデータは、Apache Cassandra データベースに格納されます。オプションのデータベース ソフトウェアを設定して、パフォーマンス メトリックを格納および取得する方法の詳細については、 [履歴メトリック データを格納するための Cassandra データベースのインストールと構成](#)を参照してください。

vCloud Director と Apache Cassandra データベース間の接続を作成するには、次の形式でコマンド ラインを使用します。

```
cell-management-tool cassandra options
```

表 10-15. セル管理ツールのオプションと引数、cassandra サブコマンド

コマンド	引数	説明
<code>--help (-h)</code>	なし	このコマンドで使用可能なオプションの概要を示します。
<code>--add-rollup</code>	なし	メトリック スキーマを更新し、集計メトリックを含めます。 <a href="#">履歴メトリック データを格納するための Cassandra データベースのインストールと構成</a> を参照してください。
<code>--cluster-nodes</code>	<code>address [, address ... ]</code>	vCloud Director メトリックで使用する Cassandra クラスター ノードのカンマ区切りのリストです。
<code>--clean</code>	なし	Cassandra 設定を vCloud Director データベースから削除します。
<code>--configure</code>	なし	既存の Cassandra クラスターで使用する vCloud Director を構成します。
<code>--dump</code>	なし	現在の接続の設定をダンプします。

表 10-15. セル管理ツールのオプションと引数、cassandra サブコマンド（続き）

コマンド	引数	説明
--keyspace	文字列	Cassandra の vCloud Director キースペース名を <i>string</i> に設定します。デフォルトでは <i>vcloud_metrics</i> です。
--offline	なし	vCloud Director で使用するために Cassandra を設定しますが、vCloud Director に接続して設定をテストすることはありません。
--password	文字列	Cassandra データベース ユーザーのパスワード
--port	整数	各クラスター ノードに接続するためのポート。デフォルトでは 9042 です。
--ttl	整数	<i>integer</i> 日間、メトリック データを保持します。メトリック データを永続的に保持するには、 <i>integer</i> を 0 に設定します。
--update-schema	なし	vCloud Director メトリック データを保持するため、Cassandra スキーマを初期化します。
--username	文字列	Cassandra データベース ユーザーのユーザー名。

## 例：Cassandra データベース接続の設定

次のようなコマンドを使用します。ここで、*node1-ip*、*node2-ip*、*node3-ip*、および *node4-ip* は Cassandra クラスターのメンバーの IP アドレスです。デフォルトのポート (9042) が使用されます。メトリック データは 15 日間保持されます。

```
[root@cell1 /opt/vmware/vcloud-director/
bin]# ./cell-management-tool cassandra --configure --create-schema \
--cluster-nodes node1-ip,node2-ip,node3-ip, node4-ip \
--username admin --password 'P@55w0rd' --ttl 15
```

このコマンドが完了した後、セルを再起動する必要があります。

## システム管理者のパスワードの復元

vCloud Director データベースのユーザー名とパスワードが分かっている場合は、セル管理ツールの *recover-password* コマンドを使用して、vCloud Director システム管理者のパスワードを復元できます。

セル管理ツールの *recover-password* コマンドでは、vCloud Director データベースのユーザー名とパスワードを知っているユーザーが、vCloud Director システム管理者のパスワードを復元できます。

システム管理者のパスワードを復元するには、次の形式でコマンドラインを使用します。

```
cell-management-tool recover-password options
```

表 10-16. セル管理ツールのオプションと引数、recover-password サブコマンド

オプション	引数	説明
--help (-h)	なし	このカテゴリで使用可能なコマンドの概要を示します。
--dbuser	vCloud Director データベース ユーザーのユーザー名。	コマンドラインで指定する必要があります。
--dbpassword	vCloud Director データベース ユーザーのパスワード。	指定しない場合に入力が求められます。

## タスクの失敗ステータスの更新

セルが意図的にシャットダウンされたときに実行していたタスクに関連する完了ステータスを更新するには、セル管理ツールの `fail-tasks` コマンドを使用します。すべてのセルをシャットダウンしない限り、`fail-tasks` コマンドを使用することはできません。

`cell-management-tool -q` コマンドを使用してセルを静止すると、実行中のタスクは数分以内に安全に終了します。休止したセルでタスクが実行し続ける場合、スーパーユーザーはセルをシャットダウンすることができ、その結果実行しているタスクは失敗します。シャットダウンにより実行中のタスクが失敗した後、スーパーユーザーは `cell-management-tool fail-tasks` を実行してそれらのタスクの完了ステータスを更新することができます。これはタスクの完了ステータスを更新するオプションの方法ですが、管理アクションによって発生した失敗を明確に特定できるため、システムの整合性を維持するのに役立ちます。

休止したセルで実行し続けるタスクのリストを生成するには、次の形式でコマンドラインを使用します。

```
cell-management-tool -u sysadmin-username cell --status-verbose
```

表 10-17. セル管理ツールのオプションと引数、fail-tasks サブコマンド

コマンド	引数	説明
--help (-h)	なし	このカテゴリで使用可能なコマンドの概要を示します。
--message (-m)	メッセージ テキスト。	タスク完了ステータスに含めるメッセージ テキスト。

## 例：セルで実行中のタスクの終了

この例では、セルがシャットダウンされた時に実行していたタスクに関連するタスク完了ステータスを更新します。

```
[root@cell1 /opt/vmware/vcloud-director/
bin]# ./cell-management-tool fail-tasks -m "administrative shutdown"
Operation: IMPORT_SINGLETON_VAPP, Start time: 12/16/13 6:41 PM, Username: system, Organization: org1
Would you like to fail the tasks listed above?
```

「y」を入力すると、タスクが更新され、**管理シャットダウン**のステータスが完了になります。「n」と入力すると、タスクの実行を継続できます。

**注：** 応答内で複数のタスクが返された場合は、すべてのタスクを終了させるのか、それとも何も行わないのかを決定する必要があります。タスクの一部を選択して終了させることはできません。

## 監査メッセージ処理の構成

システムが監査メッセージをログに記録する方法を構成するには、セル管理ツールの `configure-audit-syslog` コマンドを使用します。

各 vCloud Director セル内のサービスは、監査メッセージを vCloud Director データベースにログとして記録し、メッセージは 90 日間保存されます。監査メッセージの保存期間を長くするには、監査メッセージを vCloud Director データベースだけでなく Linux syslog ユーティリティに送信するように vCloud Director サービスを構成します。

システム構成スクリプトでは、監査メッセージの処理方法を指定できます。『vCloud Director インストールおよびアップグレード ガイド』の「ネットワークおよびデータベース接続の構成」を参照してください。システム構成時に指定したログ記録のオプションは、2 つのファイル `global.properties` および `responses.properties` に保存されます。この 2 つのファイルに保存された監査メッセージのログ記録構成を変更するには、次の形式のセル管理ツールコマンドラインを使用します。

```
cell-management-toolconfigure-audit-syslog options
```

このセル管理ツール サブコマンドで実行した変更はすべて、セルの `global.properties` ファイルおよび `responses.properties` ファイルに保存されます。変更内容はセルの再起動後に有効になります。

表 10-18. セル管理ツールのオプションと引数、`configure-audit-syslog` サブコマンド

オプション	引数	説明
<code>--help (-h)</code>	なし	このカテゴリで使用可能なコマンドの概要を示します。
<code>--disable (-d)</code>	なし	<code>syslog</code> に対する監査イベントのログ記録を無効にします。監査イベントを vCloud Director データベースにのみログ記録します。このオプションを指定すると、 <code>global.properties</code> および <code>responses.properties</code> の <code>audit.syslog.host</code> および <code>audit.syslog.port</code> プロパティの値が設定解除されます。
<code>--syslog-host (-loghost)</code>	syslog サーバ ホストの IP アドレスまたは完全修飾ドメイン名	このオプションを指定すると、 <code>audit.syslog.host</code> プロパティの値が、指定したアドレスまたは完全修飾ドメイン名に設定されます。
<code>--syslog-port (-logport)</code>	0~65535 の整数	このオプションを指定すると、 <code>audit.syslog.port</code> プロパティの値が、指定した整数に設定されます。

--syslog-host、--syslog-port、またはその両方の値を指定した場合、コマンドでは指定した値の形式が正しいかどうかは検証されますが、指定したホストとポートの組み合わせでネットワークにアクセスできるかどうか、または実行中の syslog サービスが存在するかどうかは確認されません。

## 例：syslog サーバのホスト名を変更する

**重要：** このコマンドを使用して実行した変更は、グローバル構成ファイルと応答ファイルに書き込まれます。このコマンドを使用する前に、応答ファイルが所定の場所 (/opt/vmware/vcloud-director/etc/responses.properties) にあって書き込み可能であることを確認してください。『vCloud Director インストールおよびアップグレード ガイド』の「応答ファイルの保護と再使用」を参照してください。

syslog メッセージの送信先ホストを変更するには、次のようなコマンドを使用します。

```
[root@cell1 /opt/vmware/vcloud-director/bin]#
cell-management-tool configure-audit-syslog --loghost syslog.example.com
Using default port 514
```

この例では、新しいホストがデフォルトのポートで syslog メッセージを待機しているものと仮定しています。

このコマンドを実行すると、global.properties および responses.properties が更新されますが、変更内容はセルの再起動後に有効になります。

## 電子メール テンプレートの構成

電子メール アラートを作成する際にシステムが使用するテンプレートを管理するには、セル管理ツールの manage-email コマンドを使用します。

システムは、システム管理者の介入を必要とする可能性が高いイベントや条件をシステム管理者に通知する電子メール アラートを送信するようにデフォルトで構成されています。電子メールの受信者リストは、vCloud API または Web コンソールを使用して更新できます。次の形式のセル管理ツール コマンド ラインを使用して、各種アラートのデフォルトの電子メールの内容をオーバーライドできます。

```
cell-management-tool manage-email options
```

表 10-19. セル管理ツールのオプションと引数、manage-email サブコマンド

オプション	引数	説明
--help	なし	このカテゴリで使用可能なコマンドの概要を示します。
--delete	テンプレート名	削除するテンプレートの名前。
--lookup	テンプレート名	この引数は省略可能です。この引数を省略すると、すべてのテンプレート名の一覧が返されます。

表 10-19. セル管理ツールのオプションと引数、manage-email サブコマンド（続き）

オプション	引数	説明
--locale	テンプレート ロケール	デフォルトでは、en-US ロケールのテンプレートが操作対象になります。en-US 以外のロケールを指定する場合は、このオプションを使用します。
--set-template	更新された電子メール テンプレートの格納先ファイルのパス名	このファイルは、ローカル ホストでアクセス可能であり、なおかつユーザー vcloud.vcloud によって読み取り可能である必要があります。例：/tmp/my-email-template.txt

## 例： メール テンプレートを更新する

次のコマンドでは、DISK\_STORAGE\_ALERT\_VDCS 電子メール テンプレートの現在の内容を、/tmp/DISK\_STORAGE\_ALERT\_VDCS-new.txt という名前のファイルに作成した内容で置き換えています。

```
[root@cell1 /opt/vmware/vcloud-director/
bin]#./cell-management-tool manage-email --set-template DISK_STORAGE_ALERT_VDCS /tmp/
DISK_STORAGE_ALERT_VDCS-new.txt

New property being stored: Property "email.template.DISK_STORAGE_ALERT_VDCS.en-US" has value
"This is an alert from $productName The $datastore is used by the following PVDC(s): $pvdcList
"

Property "email.template.DISK_STORAGE_ALERT_VDCS.en-US" has value "This is an alert from $productName
The $datastore is used by the followingProvider VDC(s): $pvdcList
"

VCD Email notification details:
name                : DISK_STORAGE_ALERT_VDCS
description         : Alert when used disk storage exceeds threshold
config key          : email.template.DISK_STORAGE_ALERT_VDCS.en-US
template placeholders : [productName, storageContainerType, datastore, percentage,
currentFreeSpaceMB, diskSizeBytes, pvdcList]
template content    : This is an alert from $productName The $datastore is used by the
followingProvider VDC(s): $pvdcList
```

## 親なしの仮想マシンの検索

セル管理ツールの find-orphan-vms コマンドを使用すると、vCenter データベースには存在するが vCloud Director データベースには存在しない仮想マシンへの参照を検索できます。

vCenter データベースでは参照されているが、vCloud Director データベースでは参照されていない仮想マシンは、コンピューティング リソースおよびストレージ リソースを使用するものの vCloud Director からアクセスできないため、親なしの仮想マシンと見なされます。このような参照の不一致は、高負荷のワークロード、多数のデータベース エラーや管理アクションなど、さまざまな原因で発生します。find-orphan-vms コマンドを使用すると、

こうした親なしの仮想マシンを一覧表示して、vCloud Director から削除したり、vCloud Director に再インポートしたりできます。このコマンドには、別のトラスト ストアを指定するためのオプションが用意されています。このオプションは、自己署名証明書を使用している vCloud Director または vCenter インストール環境で作業する場合に必要なことがあります。

コマンドの形式は次のとおりです。

```
cell-management-tool find-orphan-vm options
```

表 10-20. セル管理ツールのオプションと引数、find-orphan-vm サブコマンド

オプション	引数	説明
--help (-h)	なし	このカテゴリで使用可能なコマンドの概要を示します。
--enableVerifyHostname	なし	SSL ハンドシェイクのホスト名検証部分を有効にします。
--host	必須	親なしの仮想マシンの検索対象となる vCloud Director インストール先の IP アドレスまたは完全修飾ドメイン名。
--output-file	パス名または -	親なしの仮想マシンのリストの出力先となるファイルのフル パス名。リストを標準出力に書き込む場合は、パス名に - を指定します。
--password (-p)	必須	vCloud Director システム管理者のパスワード。
--port	vCloud Director の HTTPS ポート。	このオプションは、デフォルトの vCloud Director HTTPS ポートを使用しない場合のみ指定します。
--trustStore	Java トラスト ストア ファイルへのフル パス名。	このオプションは、デフォルトの vCloud Director トラスト ストア ファイルを使用しない場合のみ指定します。
--trustStorePassword	指定した --trustStore のパスワード	--trustStore を使用して別のトラスト ストア ファイルを指定した場合のみ必要です。
--trustStoreType	指定した --trustStore のタイプ (PKCS12、JCEKS など)	--trustStore を使用して別のトラスト ストア ファイルを指定した場合のみ必要です。
--user (-u)	必須	vCloud Director システム管理者のユーザー名。
--vc-name	必須	親なしの仮想マシンの検索対象 vCenter の名前。
--vc-password	必須	vCenter 管理者のパスワード。
--vc-user	必須	vCenter 管理者のユーザー名。



## 例：親なしの仮想マシンの検索

この例では、単一の vCenter Server にクエリを発行しています。--output-file オプションに - が指定されているため、クエリ結果は標準出力に返されます。

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./cell-management-tool find-orphan-vm \
--host 10.20.30.40 -u vadmin -vc-name vcenter1 -vc-password P055w0rd --vc-user admin --output-file -
Querying for VC by name 10.20.30.40
Querying all vdc's associated with VC: 10.20.30.40 (https://10.20.30.40:443)
Querying all vdc->resource pool mappings associated with VC: 10.20.30.40 (https://10.20.30.40:443)
Querying all vdc->VM Moref mappings associated with VC: 10.20.30.40 (https://10.20.30.40:443)
Processing 956 VM's on 5 VDC's across 20 resource pools
Analysis complete.
VDC: "ExampleOrgVDC [urn:vcloud:vdc:1a97...]" (org: "ExampleOrg") ResPool: primary (1a97...) [moref:
"resgroup-30515"]
The following 22 orphan VMs were discovered:
Orphan VM: "indDisk100-0-95411 (cbc358a0-e199-4024-8fff-2e5cfce20953)" (parent name: "Test VMs",
parent moref : "group-v30533")
...
Orphan VM: "indDisk12-0-51259 (0bbb4115-673e-4c84-ba26-6875159655e0)" (parent name: "Test VMs",
parent moref : "group-v30533")
```

## VMware カスタマ エクスペリエンス改善プログラムへの参加または離脱

VMware カスタマ エクスペリエンス改善プログラムに参加または離脱するには、セル管理ツールの `configure-ceip` サブコマンドを使用します。

この製品は、VMware のカスタマ エクスペリエンス改善プログラム（「CEIP」）に参加しています。CEIP を通じて収集されるデータについての詳細と、VMware がこの情報を使用する目的は、Trust & Assurance Center (<http://www.vmware.com/trustvmware/ceip.html>) で説明されています。セル管理ツールを使用して、この製品の VMware CEIP への参加または離脱をいつでも実行できます。

```
cell-management-tool
configure-ceip
options
```

この製品の CEIP に参加しない場合は、--disable オプションを指定してこのコマンドを実行します。

表 10-21. セル管理ツールのオプションと引数、 `configure-ceip` サブコマンド

オプション	引数	説明
--help (-h)	なし	このカテゴリで使用可能なコマンドの概要を示します。
--disable	なし	VMware カスタマ エクスペリエンス改善プログラムから離脱します。

表 10-21. セル管理ツールのオプションと引数、configure-ceip サブコマンド（続き）

オプション	引数	説明
--enable	なし	VMware カスタマ エクスペリエンス改善プログラムに参加します。
--status	なし	VMware カスタマ エクスペリエンス改善プログラムに対する現在の参加ステータスを表示します。

## 例： VMware カスタマ エクスペリエンス改善プログラムから離脱します。

VMware カスタマ エクスペリエンス改善プログラムから離脱するには、次のようなコマンドを使用します。

```
[root@cell1 /opt/vmware/vcloud-director/
bin]#cell-management-tool configure-ceip --disableParticipation disabled
```

このコマンドを実行すると、VMware カスタマ エクスペリエンス改善プログラムに対して情報が送信されなくなります。

VMware カスタマ エクスペリエンス改善プログラムに対する現在の参加ステータスを確認するには、次のようなコマンドを使用します。

```
[root@cell1 /opt/vmware/vcloud-director/
bin]#cell-management-tool configure-ceip --statusParticipation disabled
```

## アプリケーションの設定の更新

セル管理ツールの manage-config サブコマンドを使用すると、カタログ スロットリング アクティビティなどのさまざまなアプリケーションの構成を更新できます。

表 10-22. セル管理ツールのオプションと引数、manage-config サブコマンド

オプション	引数	説明
--help(-h)	なし	このサブコマンドで使用可能なオプションの概要を示します。
--delete(-d)	なし	ターゲットの設定を削除します。
--lookup(-l)	なし	ターゲットの設定の値を検索します。
--name(-n)	設定名	ターゲットの設定の名前。 オプション -d、-l、および -v が必要です。
--value(-v)	設定値	ターゲットの設定の値を追加または更新します。

たとえば、[カタログ同期のスロットリングの設定](#)には manage-config サブコマンドを使用できます。

## カタログ同期のスロットリングの設定

他の組織に公開された、または他の組織からサブスクライブされたカタログ項目が多数ある場合、カタログの同期中にシステムが過負荷にならないように、カタログ同期のスロットリングを設定できます。セル管理ツールの `manage-config` サブコマンドを使用すると、同時に同期できるライブラリ項目の数を制限することで、カタログ同期のスロットリングを設定できます。

サブスクライブされたカタログがカタログ同期を開始すると、公開されたカタログは最初にライブラリ項目を vCenter Server リポジトリから vCloud Director 転送サービス ストレージにダウンロードしてから、サブスクライブされたカタログのダウンロード リンクを作成します。公開されたすべてのカタログが同時にダウンロードできるライブラリ項目の数を制限できます。サブスクライブされたすべてのカタログが同時に同期できるライブラリ項目の数を制限できます。サブスクライブされた単一のカタログが同時に同期できるライブラリ項目の数を制限できます。

セル管理ツールの `manage-config` サブコマンドを使用すると、カタログ スロットリングの設定を更新できます。`manage-config` サブコマンドの使用方法については、[アプリケーションの設定の更新](#) を参照してください。

表 10-23. カタログ スロットリングの設定

設定	デフォルト値	説明
<code>vcloud.tasks.VDC_ENABLE_DOWNLOAD.queue.limit</code>	30	<p>vCloud Director インスタンス内で公開されたすべてのカタログが vCenter Server から vCloud Director に同時にダウンロードできるライブラリ項目の制限値。</p> <p>vCloud Director インスタンスをまたがってダウンロードする公開されたライブラリ項目の合計数がこの制限値を超えると、ライブラリ項目はこの制限値によって分割され、順番にダウンロードされます。</p>
<code>vcloud.tasks.LIBRARY_ITEM_SYNC.queue.limit</code>	30	<p>vCloud Director インスタンス内のサブスクライブされたすべてのカタログが同時に同期できるライブラリ項目の制限値。</p> <p>vCloud Director インスタンスをまたがって同期するサブスクライブされたライブラリ項目の合計数がこの制限値を超えると、項目はこの制限値によって分割され、順番に同期されます。</p>
<code>contentLibrary.item.sync.batch.size</code>	10	<p>サブスクライブされた単一のカタログが同時に同期できるライブラリ項目の制限値。</p> <p>サブスクライブされたカタログがこの制限値を超える数のライブラリ項目を同期すると、項目はこの制限値によって分割され、順番に同期されます。</p>

## 例：サブスクライブされたカタログの同期のロットリングの設定

次のコマンドは、サブスクライブされた単一のカタログが同時に同期できるライブラリ項目の制限値を 5 に設定します。

```
[root@cell1 /opt/vmware/vcloud-director/
bin]#./cell-management-tool manage-config -n contentLibrary.item.sync.batch.size -v 5
```

サブスクライブされたカタログに 13 個のライブラリ項目が含まれている場合は、カタログの同期は 3 回に分かれて順次実行されます。最初には 5 個の項目が含まれ、2 番目の部分には次の 5 個の項目が含まれ、最後に残りの 3 個の項目が含まれます。

## vCloud Director ユーザー インターフェイスへのアクセスに失敗した場合のトラブルシューティング

vCloud Director 環境内の vCloud Director セルの有効な IP アドレスと DNS エントリを表示および更新するには、セル管理ツールの `manage-config` サブコマンドを使用します。

### 問題

ログイン成功後に、vCloud Director Service Provider Admin Portal または vCloud Director Tenant Portal にアクセスすることはできません。

ログイン画面に認証情報を入力すると、次のエラー メッセージが表示されます。「起動に失敗しました。初期化中にエラーが発生しました。このエラーは、サポート対象外のパブリック URL を使用してアプリケーションにアクセスしている、または接続に問題が発生していることが原因であることがあります。」

### 原因

vCloud Director は、Cross-Origin Resource Sharing (CORS) フィルタの実装を使用して、Service Provider Admin Portal および vCloud Director Tenant Portal にアクセスする際に使用できる有効なすべてのエンドポイントのリストを維持します。

CORS フィルタ リストは、セルの設定中に入力および更新されます。このリストには、サーバ グループ内のすべてのセルの IP アドレスと DNS 名を含む HTTP および HTTPS エントリが格納されています。また、vCloud Director サーバ グループにあるロード バランサで使用するパブリック IP アドレスも格納されています。

アプライアンス環境のセル設定中に、vCloud Director セルの DNS 名を使用してリストが更新されることはありません。また、セルの DNS 名を使用してセルにアクセスすることはできません。

### 解決方法

- 1 サーバ グループ内のいずれかのセルに root としてログインするか、SSH で接続します。
- 2 使用環境内の vCloud Director セルにアクセスする際に使用できる有効な URL を一覧表示するには、次のコマンドラインを実行します。

```
[root@cell /opt/vmware/vcloud-director/bin]#./cell-management-tool manage-config -n
webapp.allowed.origins -l
```

システム出力は、サーバ グループ内のすべてのセルの IP アドレスと DNS 名を含む HTTP および HTTPS エントリからなるリストです。また、vCloud Director サーバ グループにあるロード バランサで使用されるパブリック IP アドレスも格納されています。

リストはカンマ区切りの文字列です。エントリの間にはスペースを含めません。

- 3 (オプション) `webapp.allowed.origins` の設定を更新するには、次のコマンド ラインを実行します。コマンド ラインでは、この設定の値パラメータに、IP アドレスと DNS 名からなるカンマ区切り文字列のリストを指定します。エントリの間にはスペースを含めません。

```
[root@cell /opt/vmware/vcloud-director/bin]#./cell-management-tool manage-config -n
webapp.allowed.origins -v "comma_separated_list_of_URLs_without_spaces"
```

## vCenter Server 仮想マシン検出のデバッグ

セル管理ツールの `debug-auto-import` サブコマンドを使用すると、vApp の検出メカニズムが vCenter Server 仮想マシンを 1 台以上スキップする原因を調査できます。

デフォルト構成の場合、組織仮想データセンターは、仮想データセンターをバックアップするリソース プールで作成される vCenter Server 仮想マシンを自動的に検出します。vApp 情報の検出および採用については、vCloud Director Service Provider Admin Portal Guide を参照してください。検出された vApp に vCenter Server 仮想マシンが表示されない場合は、この仮想マシンまたは仮想データセンターに対して `debug-auto-import` サブコマンドを実行できます。

```
cell-management-tool debug-auto-import options
```

`debug-auto-import` サブコマンドは、検出メカニズムがスキップした vCenter Server 仮想マシンのリスト、およびその潜在的な原因に関する情報を返します。このリストには、メカニズムで検出されたものの、組織仮想データセンターへのインポートに失敗した vCenter Server 仮想マシンも含まれます。

表 10-24. セル管理ツールのオプションと引数、`debug-auto-import` サブコマンド

オプション	引数	説明
<code>--help</code> ( <code>-h</code> )	なし	このカテゴリで使用可能なコマンドの概要を示します。
<code>--org</code>	組織名	オプション。指定した組織について、スキップされた仮想マシンに関する情報を一覧表示します。
<code>--vm</code>	仮想マシン名または仮想マシン名の一部	指定した仮想マシン名が含まれる、スキップされた仮想マシンに関する情報を一覧表示します。  <code>--org</code> オプションが使用されている場合は、オプションです。

## 例：仮想マシン名 test による vCenter Server 仮想マシン検出のデバッグ

以下のコマンドを実行すると、すべての組織においてスキップされた vCenter Server 仮想マシンに関する情報が返されます。

```
[root@cell1 /opt/vmware/vcloud-director/bin]#./cell-management-tool debug-auto-import -vm test
```

```
VM with name:vm22-test (09ad258c-0cb0-4f69-a0a6-201cf3fe7d6b), moref vm-50 in VC testbed-vc can be skipped for the following reasons:
```

- 1) Virtual machine is already imported in vCD or is managed by vCD
- 2) Virtual machine is created by vCD

```
VM with name:test-vm1 (32210d0d-ef64-4637-b1d6-6400743a6bd9), moref vm-44 in VC testbed-vc can be skipped for the following reasons:
```

- 1) Virtual machine is not present in a vCD managed resource pool

```
VM with name:import-test3, moref vm-52inVC testbed-vc can be skippedforthe following reasons:
```

- 1) Virtual machine autoimport is either pending,in-progress or has failed and pendingforretry

この例では、検出メカニズムでスキップされた仮想マシンで、仮想マシン名に test という文字列が含まれる 3 台の vCenter Server 仮想マシンに関する情報がシステムのアウトプットで返されます。仮想マシン import-test3 は、検出されたものの仮想データセンターへのインポートが失敗した仮想マシンの例です。

## マルチサイト拡張ネットワークの MAC アドレスの再生成

同じインストール ID で構成されている 2 つの vCloud Director サイトを関連付けると、これらのサイト間の拡張ネットワークで MAC アドレスの競合が発生する可能性があります。このような競合を回避するには、インストール ID とは異なるカスタム シードに基づいて、いずれかのサイトで MAC アドレスを再生成する必要があります。

vCloud Director の初期セットアップ中に、インストール ID を設定します。vCloud Director はインストール ID を使用して、仮想マシン ネットワーク インターフェイスの MAC アドレスを生成します。同じインストール ID で構成されている 2 つの vCloud Director インストールでは、同じ MAC アドレスが生成されることがあります。MAC アドレスが重複すると、関連付けられた 2 つのサイト間の拡張ネットワークで競合が発生する可能性があります。

同じインストール ID で構成されている、関連付けられたサイト間で拡張ネットワークを作成する前に、セル管理ツールの mac-address-management サブコマンドを使用して、いずれかのサイトで MAC アドレスを再生成する必要があります。

```
cell-management-tool mac-address-management options
```

新しい MAC アドレスを生成するには、インストール ID とは異なるカスタム シードを設定します。シードはインストール ID を上書きしませんが、データベースには 2 番目の構成パラメータとして最新のシードが保存され、インストール ID がオーバーライドされます。

mac-address-management サブコマンドは、サーバ グループの任意の vCloud Director メンバーから実行します。このコマンドは vCloud Director データベースに対して実行されるため、1 つのサーバ グループに対して 1 回コマンドを実行します。

**重要：** MAC アドレスの再生成には、vCloud Director の一定のダウンタイムが必要です。再生成を開始する前に、サーバ グループ内のすべてのセルのアクティビティを休止する必要があります。

表 10-25. セル管理ツールのオプションと引数、mac-address-management サブコマンド

オプション	引数	説明
--help (-h)	なし	このカテゴリで使用可能なコマンドの概要を示します。
--regenerate	なし	<p>使用されていないすべての MAC アドレスを削除し、現在のシードに基づいて新しい MAC アドレスを生成します。これまでシードを設定したことがない場合は、MAC アドレスはインストール ID に基づいて再生成されます。使用中の MAC アドレスは保持されます。</p> <p><b>注：</b> サーバ グループ内のすべてのセルは非アクティブである必要があります。セル上のアクティビティを休止する方法については、<a href="#">セルの管理</a>を参照してください。</p>
--regenerate-with-seed	0 ～ 63 のシード番号	<p>データベースに新しいカスタム シードを設定し、使用されていないすべての MAC アドレスを削除して、新しく設定したシードに基づいて新しい MAC アドレスを生成します。使用中の MAC アドレスは保持されます。</p> <p><b>注：</b> サーバ グループ内のすべてのセルは非アクティブである必要があります。セル上のアクティビティを休止する方法については、<a href="#">セルの管理</a>を参照してください。</p>
--show-seed	なし	現在のシードと各シードに使用されている MAC アドレスの数を返します。

**重要：** 使用中の MAC アドレスは保持されます。使用中の MAC アドレスを再生成された MAC アドレスに変更するには、ネットワーク インターフェイスの MAC アドレスをリセットする必要があります。仮想マシンのプロパティの編集については、『vCloud Director Tenant Portal Guide』を参照してください。

## 例：新しいカスタム シードに基づく MAC アドレスの再生成

次のコマンドを実行すると、現在のシードを 9 に設定し、新しく設定したシードに基づいて、使用されていないすべての MAC アドレスを再生成します。

```
[root@cell1 /opt/vmware/vcloud-director/
bin]#./cell-management-tool mac-address-management --regenerate-with-seed 9
Successfully removed 65,535 unused MAC addresses.
Successfully generated new MAC addresses.
```

## 例：現在のシードと各シードに使用されている MAC アドレスの数の表示

次のコマンドを実行すると、現在のシードと各シードの MAC アドレスの数に関する情報を返します。

```
[root@cell1 /opt/vmware/vcloud-director/bin]#./cell-management-tool mac-address-management --show-seed
Current MAC address seed is '9' and based on MacAddressSeed config.
MAC address seed    9 is in use by    12 MAC addresses
MAC address seed    1 is in use by     1 MAC addresses
```

この例では、現在のシードが 9 であり、12 個の MAC アドレスで使用されていることがシステム出力に示されています。また、1 つ前のシードまたはインストール ID に基づく MAC アドレスが 1 つあることも示されています。

## vCloud Director セルのデータベース IP アドレスの更新

セル管理ツールを使用して、データベース高可用性クラスタ内の vCloud Director セルの IP アドレスを更新できます。

### 前提条件

データベース高可用性クラスタ内のセルの IP アドレスを更新するには、現在のプライマリの IP アドレスを指定する必要があります。IP アドレスを見つけるには、クラスタのステータスを確認して、プライマリ ロールを持つノードを特定します。ノードが実行されている必要があります。この行の Connection string 列のホスト値を使用して IP アドレスを特定します。[データベース高可用性クラスタのステータスの確認](#)を参照してください。

### 手順

- 1 クラスタ内のいずれかのセルの OS に、**root** としてログインするか、SSH で接続します。
- 2 セルがそのノードで実行されているかどうかを確認します。

```
service vmware-vcd pid cell
```

セルのプロセス ID が NULL でない場合は、vCloud Director セルは実行されており、vCloud Director セルを再起動せずにデータベースの IP アドレスを変更できます。

- 3 サーバ グループ内のすべてのセルの IP アドレスを更新するには、次のコマンドを実行します。

```
/opt/vmware/vcloud-director/bin/cell-management-tool reconfigure-database --database-host primary
node IP address --pid cell process ID --remote-sudo-user postgres --private-key-path /opt/vmware/
vcloud-director/id_rsa
```

システム出力は、再構成が成功したことを示します。



- 4 (オプション) 各 vCloud Director セルが正しいデータベース IP アドレスを参照しているかどうかを確認します。

```
grep "database.jdbcUrl" /opt/vmware/vcloud-director/etc/global.properties
```

システム出力は、セルが更新されたことを示します。

- 5 いずれかのセルが更新されていない場合は、次のコマンドを実行して再構成します。

- セルが実行されていない場合は、次のコマンドを実行します。

```
/opt/vmware/vcloud-director/bin/cell-management-tool reconfigure-database --database-host  
primary node IP address
```

- セルが実行されている場合は、次のコマンドを実行します。

```
/opt/vmware/vcloud-director/bin/cell-management-tool reconfigure-database --database-host  
primary node IP address -i cell process ID
```

- 6 実行されていないセルを再構成した場合は、コマンドを実行して vmware-vcd サービスを再起動します。

- a コマンドを実行してサービスを停止します。

```
/opt/vmware/vcloud-director/bin/cell-management-tool cell -i $(service vmware-vcd pid cell) -s
```

- b コマンドを実行してサービスを開始します。

```
systemctl start vmware-vcd
```

# vCloud Director のインストールまたは vCloud Director アプライアンスのデプロイ後

# 11

vCloud Director サーバ グループを作成した後、Microsoft Sysprep ファイルと Cassandra データベースをインストールできます。PostgreSQL データベースを使用している場合は、SSL を設定し、データベース上の一部のパラメータを調整できます。

vCloud Director アプライアンスの作成後、vSphere ネットワーク機能を使用して、新しいネットワーク インターフェイス カード (NIC) を追加できます。『vSphere 仮想マシン管理』ガイドの[仮想マシンへのネットワーク アダプタの追加](#)情報を参照してください。

この章には、次のトピックが含まれています。

- [Microsoft Sysprep ファイルのサーバーへのインストール](#)
- [vCloud Director アプライアンスのタイムゾーンの変更](#)
- [公開アドレスのカスタマイズ](#)
- [履歴メトリック データを格納するための Cassandra データベースのインストールと構成](#)
- [外部 PostgreSQL データベースでの追加設定の実行](#)

## Microsoft Sysprep ファイルのサーバーへのインストール

クラウドで特定の古い Microsoft オペレーティング システムに対するゲストのカスタマイズ サポートが必要な場合は、サーバ グループの各メンバーに適切な Microsoft Sysprep ファイルをインストールする必要があります。

Sysprep ファイルは、一部の古い Microsoft オペレーティング システムにのみ必要です。クラウドでこれらのオペレーティング システムのゲストのカスタマイズをサポートする必要がない場合は、Sysprep ファイルのインストールは不要です。

Sysprep バイナリ ファイルをインストールするには、それらをサーバー上の特定の場所にコピーします。サーバー グループの各メンバーに対してファイルをコピーする必要があります。

### 前提条件

Windows 2003 および Windows XP の 32 ビットおよび 64 ビットの Sysprep バイナリ ファイルにアクセスできることを確認します。

### 手順

- 1 ターゲット サーバに root としてログインします。

- 2 ディレクトリを `$VCLLOUD_HOME/guestcustomization/default/windows` に変更します。

```
[root@cell1 /]# cd /opt/vmware/vcloud-director/guestcustomization/default/windows
```

- 3 `sysprep` という名前のディレクトリを作成します。

```
[root@cell1 /opt/vmware/vcloud-director/guestcustomization/default/windows]# mkdir sysprep
```

- 4 Sysprep バイナリ ファイルを必要とする各ゲスト OS に対して、`$VCLLOUD_HOME/guestcustomization/default/windows/sysprep` のサブディレクトリを作成します。

サブディレクトリ名は、ゲスト OS に特有のものとなります。

表 11-1. Sysprep ファイルのサブディレクトリの割り当て

ゲスト OS	<code>\$VCLLOUD_HOME/guestcustomization/default/windows/sysprep</code> の下に作成するサブディレクトリ
Windows 2003 (32 ビット)	svr2003
Windows 2003 (64 ビット)	svr2003-64
Windows XP (32 ビット)	xp
Windows XP (64 ビット)	xp-64

たとえば、Windows XP の Sysprep バイナリ ファイルを持つサブディレクトリを作成するには、次の Linux コマンドを使用します。

```
[root@cell1 /opt/vmware/vcloud-director/guestcustomization/default/windows]# mkdir sysprep/xp
```

- 5 サーバー グループ内の各 vCloud Director サーバー上の適切な場所に Sysprep バイナリ ファイルをコピーします。

- 6 ユーザー `vcloud.vcloud` が Sysprep ファイルを読み込めることを確認してください。

これを実行するには、Linux `chown` コマンドを使用します。

```
[root@cell1 /]# chown -R vcloud:vcloud $VCLLOUD_HOME/guestcustomization
```

## 結果

サーバー グループのすべてのメンバーに Sysprep ファイルをコピーすると、クラウド内の仮想マシン上でゲストのカスタマイズを実行できます。Sysprep ファイルのコピー後に vCloud Director を再起動する必要はありません。

## vCloud Director アプライアンスのタイムゾーンの変更

vCloud Director アプライアンスを正常にデプロイしたら、アプライアンスのシステム タイムゾーンを変更できます。サーバ グループおよび転送サーバ ストレージ内のすべての vCloud Director アプライアンス インスタンスで同じ設定を使用する必要があります。

#### 前提条件

- vCloud Director アプライアンスをデプロイします。6 章 [vCloud Director アプライアンスのデプロイ](#) を参照してください。
- 転送サーバ ストレージのタイムゾーンを vCloud Director プライマリ アプライアンスの新しいタイムゾーンに変更します。

#### 手順

- 1 プライマリ ノードの Web コンソールまたはリモート コンソールを使用して、コンソール ウィンドウの左下にある [タイムゾーンの設定] を選択します。
- 2 場所、国、およびタイムゾーン領域を選択します。  
新しく選択したタイムゾーンがコンソール ウィンドウの左下に表示されます。
- 3 vCloud Director アプライアンス コンソールに root としてログインします。
- 4 vCloud Director アプライアンスで新しいタイムゾーンが確実に使用されるようにするには、vmware-vcd サービスを再起動します。
- 5 vCloud Director 環境のすべてのスタンバイ セルおよびアプリケーション セルに[手順 1](#) ~ [手順 4](#) を繰り返します。

## 公開アドレスのカスタマイズ


ロード バランサまたはプロキシの要件を満たすには、vCloud Director Web ポータル、vCloud API、およびコンソール プロキシのデフォルトのエンドポイント Web アドレスを変更します。

vCloud Director アプライアンスはコンソール プロキシ サービスに単一の IP アドレスとカスタム ポート 8443 を使用するため、このアプライアンスをデプロイした場合は、vCloud Director 公開コンソールのプロキシ アドレスを設定する必要があります。[手順 6](#) を参照してください。

#### 前提条件

システム管理者のみが公開エンドポイントをカスタマイズできます。

#### 手順

- 1 メイン メニュー () から、[管理] を選択します。
- 2 左側のパネルの [設定] で、[公開アドレス] をクリックします。
- 3 [編集] をクリックして、公開エンドポイントをカスタマイズします。

#### 4 vCloud Director URL をカスタマイズするには、[Web ポータル] エンドポイントを編集します。

- a HTTP（非セキュア）接続用のカスタムの vCloud Director パブリック URL を入力します。
- b HTTPS（セキュア）接続用のカスタムの vCloud Director パブリック URL を入力し、[アップロード] をクリックして、そのエンドポイントの信頼チェーンを確立する証明書をアップロードします。

証明書チェーンはサービス エンドポイントで使用される証明書と一致する必要があります。この証明書は、エイリアス `consoleproxy` を使用して vCloud Director セルの各キーストアにアップロードされた証明書です。ロード バランサでコンソール プロキシ接続の SSL 終端はサポートされていません。証明書チェーンには、プライベート キーを含まない PEM 形式のエンドポイント証明書、中間証明書、およびルート証明書が含まれている必要があります。

#### 5 （オプション）vCloud REST API と OpenAPI URL をカスタマイズするには、[Web ポータル設定の使用] トグルを無効にします。

- a カスタムの HTTP ベース URL を入力します。

たとえば、HTTP ベース URL を **`http://vcloud.example.com`** に設定した場合は、`http://vcloud.example.com/api` から vCloud API に、`http://vcloud.example.com/cloudapi` から vCloud OpenAPI にアクセスできます。

- b カスタムの HTTPS REST API ベース URL を入力し、[アップロード] をクリックして、そのエンドポイントの信頼チェーンを確立する証明書をアップロードします。

たとえば、HTTPS REST API ベース URL を **`https://vcloud.example.com`** に設定した場合は、`https://vcloud.example.com/api` から vCloud API に、`https://vcloud.example.com/cloudapi` から vCloud OpenAPI にアクセスできます。

証明書チェーンはサービス エンドポイントで使用される証明書と一致する必要があります。この証明書は、エイリアス `http` を使用して vCloud Director セルの各キーストアにアップロードされた証明書、またはロード バランサの VIP 証明書（SSL 終端が使用されている場合）のいずれかになります。証明書チェーンには、プライベート キーを含まない PEM 形式のエンドポイント証明書、中間証明書、およびルート証明書が含まれている必要があります。

#### 6 カスタムの vCloud Director 公開コンソール プロキシ アドレスを入力します。

このアドレスは、ポート番号が指定された、vCloud Director サーバまたはロード バランサの完全修飾ドメイン名 (FQDN) です。デフォルト ポートは 443 です。

---

**重要：** vCloud Director アプライアンスは、コンソール プロキシ サービスに `eth0` NIC とカスタム ポート 8443 を使用します。

---

たとえば、vCloud Director アプライアンスのインスタンスの FQDN が `vcloud.example.com` の場合は、**`「vcloud.example.com:8443」`** と入力します。

vCloud Director は、仮想マシン上でリモート コンソール ウィンドウを開くときにコンソール プロキシ アドレスを使用します。

#### 7 変更内容を保存するには、[保存] をクリックします。

## 履歴メトリック データを格納するための Cassandra データベースのインストールと構成

vCloud Director は仮想マシンのパフォーマンスやクラウド内の仮想マシンのリソース消費量に関する現在および過去の情報を示すメトリックを収集できます。履歴メトリックのデータは、Cassandra クラスタに格納されます。

Cassandra はオープン ソース データベースであり、これを使用してバックアップ ストアを提供することで、仮想マシンのメトリックのような、時系列データを収集するための拡張性とパフォーマンスに優れたソリューションが可能になります。vCloud Director で、仮想マシンから履歴メトリックを取得できるようにする場合は、Cassandra クラスタをインストールして構成し、cell-management-tool を使用して、クラスタを vCloud Director に接続する必要があります。現在のメトリックを取得する場合は、オプションのデータベース ソフトウェアは不要です。

### 前提条件

- オプションのデータベース ソフトウェアを構成する前に、vCloud Director がインストールおよび実行されていることを確認します。
- Cassandra にまだ慣れていない場合は、<http://cassandra.apache.org/>の資料を確認してください。
- メトリック データベースとしての使用をサポートしている Cassandra リリースのリストについては、『vCloud Director リリース ノート』を参照してください。Cassandra は <http://cassandra.apache.org/download/> からダウンロードできます。
- 次のように Cassandra クラスタをインストールし、構成します。
  - Cassandra クラスタには、2 台以上のホストにデプロイされている 4 台以上の仮想マシンを含める必要があります。
  - 2 台の Cassandra シード ノードが必要です。
  - Cassandra クライアントとノード間の暗号化を有効にします。<http://docs.datastax.com/en/cassandra/3.0/cassandra/configuration/secureSSLIntro.html> を参照してください。
  - Cassandra のユーザー認証を有効にします。<http://docs.datastax.com/en/cassandra/3.0/cassandra/configuration/secureConfigNativeAuth.html> を参照してください。
  - 各 Cassandra クラスタで Java Native Access (JNA) バージョン 3.2.7 以降を有効にします。
  - Cassandra ノード間の暗号化はオプションで使用できます。
  - Cassandra で SSL はオプションで使用できます。Cassandra で SSL を有効にしない場合は、各セル (\$VCLLOUD\_HOME/etc/global.properties) の global.properties ファイルで構成パラメータ `cassandra.use.ssl` を 0 に設定する必要があります。

## 手順

- 1 `cell-management-tool` ユーティリティを使用して、vCloud Director と、Cassandra クラスタに含まれるノード間の接続を構成します。

次のコマンド例では、*node1-ip*、*node2-ip*、*node3-ip*、および *node4-ip* は、Cassandra クラスタのメンバーの IP アドレスです。デフォルトのポート (9042) が使用されます。メトリック データは 15 日間保持されます。

```
[root@cell1 /opt/vmware/vcloud-director/
bin]# ./cell-management-tool cassandra --configure --create-schema \ --cluster-nodes node1-
ip,node2-ip,node3-ip, node4-ip \ --username admin --password 'P@55w0rd' --ttl 15
```

セル管理ツールの使用については、「[10 章 セル管理ツール リファレンス](#)」を参照してください。

- 2 (オプション) vCloud Director をバージョン 9.1 からアップデートする場合は、`cell-management-tool` を使用して、集計メトリックを格納するようにメトリック データベースを設定します。

次の例のようにコマンドを実行します。

```
[root@cell1 /opt/vmware/vcloud-director/
bin]# ./cell-management-tool cassandra --add-rollup \ --username admin --password 'P@55w0rd'
```

- 3 各 vCloud Director セルを再起動します。

## 外部 PostgreSQL データベースでの追加設定の実行

vCloud Director サーバ グループを作成した後、外部 PostgreSQL データベースを構成して vCloud Director セルからの SSL 接続を要求し、一部のデータベース パラメータを調整して最適なパフォーマンスを確保することができます。

最も安全な接続を行うには、一般的なパブリック認証局のルートに配置された完全なトラスト チェーンを含む、適切に署名された SSL 証明書が必要です。また、自己署名 SSL 証明書、またはプライベート認証局によって署名された SSL 証明書を使用することもできますが、この証明書は vCloud Director トラストストアにインポートする必要があります。

システムの仕様および要件に最適なパフォーマンスを得るには、データベースの構成とデータベースの構成ファイル内のオートバキューム パラメータを調整します。

## 手順

## 1 vCloud Director と PostgreSQL データベース間の SSL 接続を設定します。

- a 外部 PostgreSQL データベースに自己署名証明書またはプライベート証明書を使用した場合は、各 vCloud Director セルから vCloud Director トラストストアにデータベースの証明書をインポートするコマンドを実行します。

```
[root@cell1 /opt/vmware/vcloud-director/
bin]#cell-management-tool import-trusted-certificates --source path_to_self-
signed_or_private_cert
```

- b vCloud Director および PostgreSQL 間で SSL 接続を有効にするコマンドを実行します。

```
[root@cell1 /opt/vmware/vcloud-director/bin]#
cell-management-tool reconfigure-database --database-ssl true
```

--private-key-path オプションを使用して、サーバ グループ内のすべてのセルに対してコマンドを実行することができます。

```
[root@cell1 /opt/vmware/vcloud-director/bin]#
cell-management-tool reconfigure-database --database-ssl true --private-key-
path path_to_private_key
```

セル管理ツールの使用の詳細については、[10 章 セル管理ツール リファレンス](#)を参照してください。

## 2 システムの仕様に合わせて postgresql.conf ファイル内のデータベースの設定を編集します。

たとえば、16 GB のメモリを搭載したシステムの場合は、次のコードを使用できます。

```
max_connections = 500
# Set effective cache size to 50% of total memory.
effective_cache_size = 8GB
# Set shared buffers to 25% of total memory
shared_buffers = 4GB
```

## 3 要件に合わせて、postgresql.conf ファイル内の autovacuum パラメータを編集します。

通常の vCloud Director ワークロードでは、次のコードを使用できます。

```
autovacuum = on
track_counts = on
autovacuum_max_workers = 3
autovacuum_naptime = 1min
autovacuum_vacuum_cost_limit = 2400
```

アクティビティ テーブルおよび activity\_parameters テーブルにカスタムの autovacuum\_vacuum\_scale\_factor 値が設定されます。

## 次のステップ

postgresql.conf ファイルを編集した場合は、データベースを再起動する必要があります。



# vCloud Director のアップグレード

# 12

vCloud Director を新しいバージョンにアップグレードするには、サーバ グループ内のすべてのセルで vCloud Director サービスをシャットダウンし、各サーバに新しいバージョンをインストールし、vCloud Director データベースをアップグレードしてから、vCloud Director セルを再起動します。

既存の vCloud Director サーバ グループが Linux の vCloud Director インストール環境から構成される場合は、Linux 用の vCloud Director インストーラを使用して環境をアップグレードできます。別の方法として、環境を vCloud Director 10.0 アプライアンスに移行することもできます。[13 章 vCloud Director アプライアンスへの移行](#)を参照してください。

既存の vCloud Director サーバ グループが vCloud Director 9.5 アプライアンス環境で構成されている場合は、環境を vCloud Director アプライアンスの新しいバージョンに移行することのみが可能です。Linux 用の vCloud Director インストーラを使用した既存の環境のアップグレードは、移行ワークフローの一環としてのみ可能になります。[vCloud Director アプライアンスへの移行](#)を参照してください。

Linux に vCloud Director がインストールされている場合は、組織的なアップグレードを実行するか、手動で vCloud Director をアップグレードすることができます。[vCloud Director インストールの組織的なアップグレードの実行](#)または [vCloud Director インストールの手動アップグレード](#)を参照してください。組織的なアップグレードでは、サーバ グループ内のすべてのセルとデータベースをアップグレードする 1 つのコマンドを実行します。手動のアップグレードでは、各セルとデータベースを順番にアップグレードします。

vCloud Director アプライアンスのバージョン 9.7 からバージョン 10.0 へのアップグレードについては、[vCloud Director アプライアンスのアップグレード](#)を参照してください。

vCloud Director 9.5 以降：

- Oracle データベースはサポートされません。既存の vCloud Director インストールで Oracle データベースが使用されている場合は、[のアップグレードおよび移行パス](#)テーブルを参照してください。
- ESXi ホストの有効/無効を切り替えることはできません。アップグレードを開始する前に、ESXi のすべてのホストを有効にする必要があります。vSphere Client を使用して、ESXi ホストをメンテナンスモードにすることができます。
- vCloud Director は、Java および強化された LDAP サポートを使用します。LDAP ログインの失敗を回避するために LDAPS サーバを使用している場合は、適切に構築された証明書があることを確認する必要があります。詳細については、<https://www.java.com> の「Java 8 Release Changes」を参照してください。

vCloud Director 10.0 以降では、Microsoft SQL Server データベースはサポートされません。

vCloud Director をアップグレードする場合は、新しいバージョンと、既存インストールの以下のコンポーネントとの間に互換性が必要です。

- vCloud Director データベース用に現在使用しているデータベース ソフトウェア。詳細については、「アップグレードと移行のパス」テーブルを参照してください。
- 現在使用している VMware vSphere® リリース。
- 現在使用している VMware NSX® リリース。
- vCloud Director と直接通信するサードパーティ製コンポーネント。

vCloud Director と他の VMware 製品およびサードパーティ製データベースとの互換性については、[http://partnerweb.vmware.com/comp\\_guide/sim/interop\\_matrix.php](http://partnerweb.vmware.com/comp_guide/sim/interop_matrix.php) にある VMware 製品の相互運用性マトリックスを参照してください。vCloud Director アップグレードの一環として vSphere または NSX コンポーネントをアップグレードする場合は、vCloud Director をアップグレードした後にこれらをアップグレードする必要があります。14 章 [vCloud Director をアップグレードまたは移行した後に行う作業](#) を参照してください。

1 台以上の vCloud Director サーバをアップグレードしてから、vCloud Director データベースをアップグレードできます。データベースには、サーバーで実行されているすべての vCloud Director タスクの状態を含む、サーバーのランタイム状態に関する情報が保存されます。アップグレード後に無効なタスク情報がデータベース内に残らないようにするため、アップグレードを開始する前に、どのサーバにもアクティブなタスクがないことを確認する必要があります。

アップグレードでは、vCloud Director データベースに格納されない次のアーティファクトが保持されます。

- ローカルおよびグローバルのプロパティ ファイルは新しいインストール環境にコピーされます。
- ゲスト カスタマイズに使用する Microsoft Sysprep ファイルは、新しいインストール環境にコピーされます。

アップグレードを行うには、サーバ グループとデータベース内のすべてのサーバをアップグレードするのに必要な vCloud Director のダウンタイムを確保する必要があります。ロード バランサーを使用している場合は、システムがアップグレードのためオフラインになっています (The system is offline for upgrade) のようなメッセージを返すように設定できます。

## アップグレード パスと移行パスおよびワークフロー

アップグレード元の環境	ターゲット環境	
	外部 PostgreSQL データベースを使用する Linux 上の vCloud Director 10.0	組み込みの PostgreSQL データベースを使用する vCloud Director アプライアンス 10.0
外部 Oracle データベースを使用する vCloud Director 9.0 および 9.1	<ol style="list-style-type: none"> <li>1 Linux 上の vCloud Director 9.0 の場合は、vCloud Director をバージョン 9.1 にアップグレードします。<a href="#">vCloud Director のアップグレード</a>を参照してください。</li> <li>2 Oracle データベースを PostgreSQL データベースに移行します。<a href="#">PostgreSQL データベースへの移行</a>を参照してください。</li> <li>3 環境を Linux 上の vCloud Director 10.0 にアップグレードします。<a href="#">vCloud Director インストールの組織的なアップグレードの実行</a>または <a href="#">vCloud Director インストールの手動アップグレード</a>を参照してください。</li> </ol>	<ol style="list-style-type: none"> <li>1 Linux 上の vCloud Director 9.0 の場合は、vCloud Director をバージョン 9.1 にアップグレードします。<a href="#">vCloud Director のアップグレード</a>を参照してください。</li> <li>2 Oracle データベースを PostgreSQL データベースに移行します。<a href="#">PostgreSQL データベースへの移行</a>を参照してください。</li> <li>3 環境を Linux 上の vCloud Director 10.0 にアップグレードします。<a href="#">vCloud Director インストールの組織的なアップグレードの実行</a>または <a href="#">vCloud Director インストールの手動アップグレード</a>を参照してください。</li> <li>4 vCloud Director アプライアンス 10.0 に移行します。<a href="#">外部 PostgreSQL データベースを使用する vCloud Director の vCloud Director アプライアンスへの移行</a>を参照してください。</li> </ol>
外部 PostgreSQL データベースを使用する vCloud Director アプライアンス 9.5	サポート対象外	<ol style="list-style-type: none"> <li>1 環境を Linux 上の vCloud Director 10.0 にアップグレードします。<a href="#">vCloud Director インストールの組織的なアップグレードの実行</a>または <a href="#">vCloud Director インストールの手動アップグレード</a>を参照してください。</li> <li>2 vCloud Director アプライアンス 10.0 に移行します。<a href="#">外部 PostgreSQL データベースを使用する vCloud Director の vCloud Director アプライアンスへの移行</a>を参照してください。</li> </ol>
外部 PostgreSQL データベースを使用する Linux 上の vCloud Director 9.0、9.1、9.5	環境を Linux 上の vCloud Director 10.0 にアップグレードします。 <a href="#">vCloud Director インストールの組織的なアップグレードの実行</a> または <a href="#">vCloud Director インストールの手動アップグレード</a> を参照してください。	<ol style="list-style-type: none"> <li>1 環境を Linux 上の vCloud Director 10.0 にアップグレードします。<a href="#">vCloud Director インストールの組織的なアップグレードの実行</a>または <a href="#">vCloud Director インストールの手動アップグレード</a>を参照してください。</li> <li>2 vCloud Director アプライアンス 10.0 に移行します。<a href="#">外部 PostgreSQL データベースを使用する vCloud Director の vCloud Director アプライアンスへの移行</a>を参照してください。</li> </ol>

アップグレード元の環境	ターゲット環境	
	外部 PostgreSQL データベースを使用する Linux 上の vCloud Director 10.0	組み込みの PostgreSQL データベースを使用する vCloud Director アプライアンス 10.0
外部 Microsoft SQL Server データベースを使用する Linux 上の vCloud Director 9.0、9.1、9.5	<ol style="list-style-type: none"> <li>1 環境を Linux 上の vCloud Director 9.7 にアップグレードします。<a href="#">vCloud Director のアップグレード</a>を参照してください。</li> <li>2 Microsoft SQL Server データベースを PostgreSQL データベースに移行します。<a href="#">PostgreSQL データベースへの移行</a>を参照してください。</li> <li>3 環境を Linux 上の vCloud Director 10.0 にアップグレードします。<a href="#">vCloud Director インストールの組織的なアップグレードの実行</a>または<a href="#">vCloud Director インストールの手動アップグレード</a>を参照してください。</li> </ol>	<ol style="list-style-type: none"> <li>1 環境を Linux 上の vCloud Director 9.7 にアップグレードします。<a href="#">vCloud Director のアップグレード</a>を参照してください。</li> <li>2 vCloud Director アプライアンス 9.7 に移行します。<a href="#">外部 Microsoft SQL データベースを使用する vCloud Director の vCloud Director アプライアンスへの移行</a>を参照してください。</li> <li>3 環境を vCloud Director アプライアンス 10.0 にアップグレードします。<a href="#">vCloud Director アプライアンスのアップグレード</a>を参照してください。</li> </ol>
外部 Microsoft SQL Server データベースを使用する Linux 上の vCloud Director 9.7	<ol style="list-style-type: none"> <li>1 Microsoft SQL Server データベースを PostgreSQL データベースに移行します。<a href="#">PostgreSQL データベースへの移行</a>を参照してください。</li> <li>2 環境を Linux 上の vCloud Director 10.0 にアップグレードします。<a href="#">vCloud Director インストールの組織的なアップグレードの実行</a>または<a href="#">vCloud Director インストールの手動アップグレード</a>を参照してください。</li> </ol>	<ol style="list-style-type: none"> <li>1 vCloud Director アプライアンス 9.7 に移行します。<a href="#">外部 Microsoft SQL データベースを使用する vCloud Director の vCloud Director アプライアンスへの移行</a>を参照してください。</li> <li>2 環境を vCloud Director アプライアンス 10.0 にアップグレードします。<a href="#">vCloud Director アプライアンスのアップグレード</a>を参照してください。</li> </ol>
外部 PostgreSQL データベースを使用する Linux 上の vCloud Director 9.7	環境を Linux 上の vCloud Director 10.0 にアップグレードします。 <a href="#">vCloud Director インストールの組織的なアップグレードの実行</a> または <a href="#">vCloud Director インストールの手動アップグレード</a> を参照してください。	<ol style="list-style-type: none"> <li>1 vCloud Director アプライアンス 9.7 に移行します。<a href="#">Migrating vCloud Director with an External PostgreSQL Database to vCloud Director Appliance</a>を参照してください。</li> <li>2 環境を vCloud Director アプライアンス 10.0 にアップグレードします。<a href="#">vCloud Director アプライアンスのアップグレード</a>を参照してください。</li> </ol>
組み込みの PostgreSQL データベースを使用する vCloud Director アプライアンス 9.7	サポート対象外	環境を vCloud Director アプライアンス 10.0 にアップグレードします。 <a href="#">vCloud Director アプライアンスのアップグレード</a> を参照してください。
外部 PostgreSQL データベースを使用する Linux 上の vCloud Director 10.0	該当なし	vCloud Director アプライアンス 10.0 に移行します。 <a href="#">外部 PostgreSQL データベースを使用する vCloud Director の vCloud Director アプライアンスへの移行</a> を参照してください。

この章には、次のトピックが含まれています。

- [vCloud Director アプライアンスのアップグレード](#)
- [アップグレードが失敗した場合の vCloud Director アプライアンスのロールバック](#)
- [VMware Update Repository を使用した vCloud Director アプライアンスのアップグレード](#)
- [vCloud Director インストールの組織的なアップグレードの実行](#)
- [vCloud Director インストールの手動アップグレード](#)
- [データベース アップグレード ユーティリティ リファレンス](#)

## vCloud Director アプライアンスのアップグレード

vCloud Director アプライアンスをバージョン 9.7 からバージョン 10.0 にアップグレードするか、vCloud Director 10.0 をパッチ リリースにアップグレードすることができます。

vCloud Director アプライアンス環境へのアップグレード中に vCloud Director サービスは動作を停止し、一定時間のダウンタイムが発生すると予想されます。ダウンタイムは、各 vCloud Director アプライアンスをアップグレードし、vCloud Director データベース アップグレード スクリプトを実行するための所要時間によって異なります。最後の vCloud Director アプライアンスで vCloud Director サービスを停止するまで、vCloud Director サーバ グループ内の動作中のセルの数は減少します。vCloud Director HTTP エンドポイントの前に配置された、適切に構成されたロード バランサで、停止されたセルへのトラフィックのルーティングを停止する必要があります。

すべての vCloud Director アプライアンスにアップグレードを適用し、データベースのアップグレードが完了したら、各 vCloud Director アプライアンスを再起動する必要があります。

### 前提条件

プライマリ vCloud Director アプライアンスのスナップショットを作成します。

- 1 データベース高可用性クラスタのプライマリ vCloud Director アプライアンスが配置されている vCenter Server インスタンスにログインします。
- 2 プライマリ vCloud Director アプライアンスに移動して右クリックし、[パワー] - [ゲスト OS をシャットダウン] をクリックします。
- 3 アプライアンスを右クリックして、[スナップショット] - [スナップショットの作成] をクリックします。スナップショットの名前と、必要に応じて説明を入力し、[OK] をクリックします。
- 4 vCloud Director アプライアンスを右クリックし、[パワー] - [パワーオン] をクリックします。
- 5 データベース高可用性構成に含まれているすべてのノードが良好な状態であることを確認します。[データベース高可用性クラスタのステータスの確認](#)を参照してください。

### 手順

- 1 Web ブラウザで、vCloud Director アプライアンス インスタンスのアプライアンス管理ユーザー インターフェイスにログインして、プライマリ アプライアンス `https://appliance_ip_address:5480` を特定します。

プライマリ アプライアンス名を書き留めておきます。スタンバイ セルとアプリケーション セルの前にプライマリ アプライアンスをアップグレードする必要があります。データベースをバックアップする場合は、プライマリ アプライアンスを使用する必要があります。

- 2 アップデート パッケージを、アップグレードするアプライアンスにダウンロードします。

**注：** 最初にプライマリ アプライアンスをアップグレードする必要があります。

vCloud Director は VMware\_vCloud\_Director\_v という形式の名前で実行可能ファイルとして配布されます。  
v.v.v-*nnnnnnnn*\_update.tar.gz。v.v.v.v は製品バージョン、*nnnnnnnn* はビルド番号を表します。たとえば、VMware\_vCloud\_Director\_10.0.0.4424-14420378\_update.tar.gz のようになります。

- 3 アップデート パッケージを抽出する local-update-package ディレクトリを作成します。

```
mkdir /tmp/local-update-package
```

- 4 新しく作成したディレクトリにアップデート パッケージを抽出します。

```
tar -zxf VMware_vCloud_Director_v.v.v.v-nnnnnnnn_update.tar.gz \  
-C /tmp/local-update-package
```

- 5 local-update-package ディレクトリをアップデート リポジトリとして設定します。

```
vamicli update --repo file:///tmp/local-update-package
```

- 6 アップデートを調べて、リポジトリが正しく設定されていることを確認します。

```
vamicli update --check
```

アップグレード リリースが Available Update として表示されます。

- 7 次のコマンドを実行して、vCloud Director をシャットダウンします。

```
/opt/vmware/vcloud-director/bin/cell-management-tool -u <admin username> cell --shutdown
```

- 8 使用可能なアップグレードを適用します。

```
vamicli update --install latest
```

- 9 残りのスタンバイ セルとアプリケーション セルに 2 ～8 を繰り返します。

- 10 プライマリ アプライアンスから、vCloud Director アプライアンスの組み込みデータベースをバックアップします。

```
/opt/vmware/appliance/bin/create-db-backup
```

- 11 任意のアプライアンスから vCloud Director データベース upgrade ユーティリティを実行します。

```
/opt/vmware/vcloud-director/bin/upgrade
```

- 12 各 vCloud Director アプライアンスを再起動します。

```
shutdown -r now
```

## 次のステップ

- アップグレードが成功した場合は、vCloud Director アプライアンスのスナップショットを削除できます。
- アップグレードに失敗した場合は、vCloud Director アプライアンスを、アップグレード前に作成したスナップショットの状態にロールバックできます。[アップグレードが失敗した場合の vCloud Director アプライアンスのロールバック](#)を参照してください。

## アップグレードが失敗した場合の vCloud Director アプライアンスのロールバック

vCloud Director アプライアンスのアップグレードが失敗した場合は、アップグレード前に作成したアプライアンスのスナップショットを使用して、vCloud Director アプライアンスをロールバックできます。

ロールバックを開始する前に、[データベース高可用性クラスタのステータスの確認](#)に記載されている手順を実行します。クラスタ内のスタンバイ ノードのノード ID を書き留めておきます。

- 1 プライマリ vCloud Director アプライアンスを、アップグレードを開始する前に作成したスナップショットの状態に戻します。

元に戻すオプションを使用して仮想マシンのスナップショットをリストアする方法を確認してください。

vSphere 仮想マシン管理ガイドの[\[元に戻す\]を使用した仮想マシンのスナップショットのリストア](#)を参照してください。

- 2 プライマリ vCloud Director アプライアンス セルをパワーオンします。
- 3 各 vCloud Director アプライアンス セルの OS に直接ログインするか、SSH クライアントを使用して接続します。root ユーザーとしてログインする必要があります。
- 4 すべてのアプライアンス セルで vCloud Director サービスを停止します。

```
service vmware-vcd stop
```

- 5 プライマリ vCloud Director セルを使用して、クラスタ内のセカンダリ ノードを登録解除します。
  - a プライマリ セルの OS に root として直接ログインするか、SSH クライアントを使用して接続します。
  - b ユーザーを postgres に変更します。

```
sudo -i -u postgres
```

- c コマンドを実行して、スタンバイ アプライアンス セルを登録解除します。

実行されていないスタンバイ ノードを登録解除するには、ノード ID を指定する必要があります。

```
/opt/vmware/vpostgres/current/bin/repmgr standby unregister --node-id=node ID -f /opt/vmware/vpostgres/current/etc/repmgr.conf
```

- d [5.c](#)を繰り返して、その他のスタンバイ アプライアンス セルを登録解除します。
- 6 vSphere Client で、すべてのスタンバイ アプライアンスをシャットダウンして削除します。
  - a vSphere Client で、スタンバイ アプライアンスに移動します。

- b スタンバイ アプライアンスを右クリックし、[パワー] - [ゲスト OS をシャットダウン] をクリックします。
  - c アプライアンスを右クリックし、[ディスクから削除] をクリックします。
  - d その他のスタンバイ アプライアンス セルに 6.a ~ 6.c を繰り返します。
- 7 プライマリ vCloud Director アプライアンス セルの repmgr ツール スイートおよび組み込みの PostgreSQL データベースが適切に機能していることを確認します。
- a ユーザーを postgres に変更します。

```
sudo -i -u postgres
```

- b コマンドを実行して、クラスタのステータスを確認します。

```
/opt/vmware/vpostgres/current/bin/repmgr cluster show
```

コンソール出力に、クラスタ内の唯一のノードに関する情報が表示されます。

ID	Name	Role	Status	Upstream	Location	Connection string
Node 1	Node name	primary	*running		default	host=host IP address user=repmgr dbname=repmgr

- 8 セカンダリ アプライアンスを再デプロイします。 [vSphere Client を使用した vCloud Director アプライアンスのデプロイ](#) を参照してください。
- 9 各 vCloud Director アプライアンス セルの OS に直接ログインするか、SSH クライアントを使用して接続します。root ユーザーとしてログインする必要があります。
- 10 vCloud Director サービスを開始します。

```
service vmware-vcd start
```

## VMware Update Repository を使用した vCloud Director アプライアンスのアップグレード

VMware Update Repository を使用すると、vCloud Director アプライアンスをバージョン 9.7 からバージョン 10.0 にアップグレードできます。

**注：** VMware Update Repository は、vCloud Director を最新バージョンの vCloud Director にアップグレードする場合にのみ使用できます。VMware Update Repository では、最新バージョンのみを使用できます。vCloud Director を別のバージョンにアップグレードする場合は、[vCloud Director アプライアンスのアップグレード](#) を参照してください。



vCloud Director アプライアンス環境へのアップグレード中に vCloud Director サービスは動作を停止し、一定時間のダウンタイムが発生すると予想されます。ダウンタイムは、各 vCloud Director アプライアンスをアップグレードし、vCloud Director データベース アップグレード スクリプトを実行するための所要時間によって異なります。最後の vCloud Director アプライアンスで vCloud Director サービスを停止するまで、vCloud Director サーバ グループ内の動作中のセルの数は減少します。vCloud Director HTTP エンドポイントの前に配置された、適切に構成されたロード バランサで、停止されたセルへのトラフィックのルーティングを停止する必要があります。

すべての vCloud Director アプライアンスにアップグレードを適用し、データベースのアップグレードが完了したら、各 vCloud Director アプライアンスを再起動する必要があります。

#### 前提条件

vCloud Director アプライアンスが <https://vapp-updates.vmware.com> にアクセスできることを確認します。

#### 手順

- 1 Web ブラウザで、vCloud Director アプライアンス インスタンスのアプライアンス管理ユーザー インターフェイスにログインして、プライマリ アプライアンス [https://appliance\\_ip\\_address:5480](https://appliance_ip_address:5480) を特定します。

プライマリ アプライアンス名を書き留めておきます。データベースをバックアップする場合は、プライマリ アプライアンスを使用する必要があります。

- 2 アップデート リポジトリをリセットして、VMware Update Repository を参照するようにします。

```
vamicli update --repo ""
```

- 3 アップデートを検索して、VMware Update Repository 内に必要なアップグレードがあることを確認します。

デフォルトでは、vamicli コマンドは VMware Update Repository を参照します。

```
vamicli update --check
```

アップグレード リリースが Available Update として表示されます。

- 4 次のコマンドを実行して、vCloud Director をシャットダウンします。

```
/opt/vmware/vcloud-director/bin/cell-management-tool -u <admin username> cell --shutdown
```

- 5 使用可能なアップグレードを適用します。

```
vamicli update --install latest
```

- 6 各アプライアンスに[手順 2](#)～[手順 4](#)を繰り返します。

- 7 プライマリ アプライアンスから、vCloud Director アプライアンスの組み込みデータベースをバックアップします。

```
/opt/vmware/appliance/bin/create-db-backup
```

- 8 任意のアプライアンスから vCloud Director データベース upgrade ユーティリティを実行します。

```
/opt/vmware/vcloud-director/bin/upgrade
```

- 9 各 vCloud Director アプライアンスを再起動します。

```
shutdown -r now
```

## vCloud Director インストールの組織的なアップグレードの実行

--private-key-path オプションを使用して vCloud Director インストーラを実行することにより、サーバ グループ内のすべてのセルと、共有データベースを同時にアップグレードできます。

Linux 用の vCloud Director インストーラを使用すると、サポート対象 Linux OS 上の vCloud Director インストール環境で構成される vCloud Director サーバ グループをアップグレードできます。vCloud Director サーバ グループが vCloud Director 9.5 アプライアンス環境で構成される場合、Linux 用の vCloud Director インストーラを使用した既存の環境のアップグレードは、移行ワークフローの一環としてのみ可能になります。[13 章 vCloud Director アプライアンスへの移行](#)を参照してください。

vCloud Director for Linux は、vmware-vcloud-director-distribution-v という形式の名前のデジタル署名された実行可能ファイルとして配布されます。v. v-nnnnnn.bin。ここで vv.v は、製品バージョン、nnnnnn はビルド番号を表します。例えば、vmware-vcloud-director-distribution-8.10.0-3698331.bin というファイル名になります。この実行可能ファイルを実行すると、vCloud Director がインストールまたはアップグレードされます。

--private-key-path オプションを指定して vCloud Director インストーラを実行する場合

は、--maintenance-cell など、upgrade ユーティリティの他のコマンド オプションを追加できます。データベースの upgrade ユーティリティのオプションの詳細については、[データベース アップグレード ユーティリティ リファレンス](#)を参照してください。

### 前提条件

- vCloud Director データベース、vSphere コンポーネント、および NSX コンポーネントが新しいバージョンの vCloud Director と互換性があることを確認します。

**重要：** 既存の vCloud Director インストールで Oracle データベースまたは Microsoft SQL Server データベースが使用されている場合は、vCloud Director バージョン 10.0 にアップグレードする前に、PostgreSQL データベースに移行したことを確認してください。使用可能なアップグレード パスについては、[12 章 vCloud Director のアップグレード](#)を参照してください。

- ターゲット サーバのスーパーユーザーの認証情報があることを確認します。
- インストーラにインストール ファイルのデジタル署名を検証させる場合、ターゲット サーバに VMware パブリック キーをダウンロードし、インストールします。インストール ファイルのデジタル署名をすでに検証している場合、インストール中にそれを再び検証する必要はありません。[VMware パブリック キーのダウンロードとインストール](#)を参照してください。
- アップグレード先の vCloud Director ソフトウェアのバージョンを使用するための有効なライセンス キーがあることを確認します。

- すべてのセルで、パスワードを要求せずにスーパー ユーザーからの SSH 接続を許可していることを確認します。検証を実行するには、次の Linux コマンドを実行します。

```
sudo -u vcloud ssh -i private-key-path root@cell-ip
```

この例では、ID が vcloud に設定され、*cell-ip* にあるセルへの SSH 接続が root として確立されますが、root パスワードの指定はありません。ローカル セルの *private-key-path* にあるプライベート キーがユーザー vcloud.vcloud から読み取り可能で、対応するパブリック キーが *cell-ip* の root ユーザーの *authorized-keys* ファイルにあれば、コマンドが成功します。

**注：** vCloud Director プロセスを実行する ID として使用するため、vCloud Director インストーラにより、vcloud ユーザー、vcloud グループ、および vcloud.vcloud アカウントが作成されます。vcloud ユーザーにはパスワードがありません。

- すべての ESXi ホストが有効であることを確認します。vCloud Director 9.5 以降では、無効な ESXi ホストはサポートされません。
- サーバ グループ内のすべてのサーバが共有された転送サーバ ストレージにアクセスできることを確認してください。[転送サーバ ストレージの準備](#)を参照してください。
- vCloud Director インストールで LDAPS サーバが使用されている場合は、アップグレード後の LDAP ログインの失敗を避けるために、Java 8 Update 181 の証明書が適切に構築されていることを確認します。詳細については、<https://www.java.com> の「Java 8 Release Changes」を参照してください。

#### 手順

- 1 ターゲット サーバに root としてログインします。

- 2 インストール ファイルをターゲット サーバーにダウンロードします。

メディアでソフトウェアを購入した場合は、ターゲット サーバからアクセス可能な場所にインストール ファイルをコピーします。

- 3 ダウンロード ページに投稿されているものとダウンロードのチェックサムが一致することを確認します。

MD5 と SHA1 チェックサムの値が、ダウンロード ページに投稿されます。適切なツールを使用して、ダウンロードされたインストール ファイルのチェックサムがダウンロード ページのものと一致することを確認します。次の形式の Linux コマンドは *installation-file* のチェックサムを表示します。

```
[root@cell1 /tmp]# md5sum installation-file
```

コマンドはインストール ファイルのチェックサムを返します。これは、ダウンロード ページの MD5 チェックサムと一致する必要があります。

- 4 インストール ファイルが実行可能であることを確認します。

インストール ファイルには実行権限が必要です。この権限を確実にインストール ファイルに設定するには、コンソール、シェル、またはターミナル ウィンドウを開き、次の Linux コマンドを実行します。*installation-file* は、vCloud Director インストール ファイルへのフル パス名です。

```
[root@cell1 /tmp]# chmod u+x installation-file
```

- 5 コンソール、シェル、またはターミナル ウィンドウで、`--private-key-path` オプションと、ターゲット セルのプライベート キーのパス名を指定して、インストール ファイルを実行します。

データベース upgrade ユーティリティの他のコマンド オプションを追加することができます。

```
./installation-file --private-key-path /vcloud/.ssh/id_rsa
```

**注：** パス名に埋め込まれたスペース文字を含むディレクトリからインストール ファイルを実行することはできません。

インストーラによって vCloud Director の以前のバージョンが検出され、アップグレードを確認するように求められます。

インストーラは、vCloud Director のバージョンが、インストール ファイル内のバージョン以降のものであることを検出すると、エラー メッセージを表示して終了します。

- 6 **y** と入力し、Enter キーを押して、アップグレードすることを確認します。

#### 結果

インストーラが以下の複数セル アップグレード ワークフローを開始します。

- 1 現在のセル ホストがすべての要件を満たしていることを確認します。
- 2 vCloud Director RPM パッケージを展開する。
- 3 現在のセルで vCloud Director ソフトウェアをアップグレードします。
- 4 vCloud Director データベースをアップグレードします。
- 5 残りのそれぞれのセルで vCloud Director ソフトウェアをアップグレードしてから、各セルで vCloud Director サービスを再起動します。
- 6 現在のセルで vCloud Director サービスを再起動します。

#### 次のステップ

サーバ グループ内のすべてのセルで vCloud Director サービスを起動します。

これで、[接続済み vCenter Server システムに関連付けられた各 NSX Manager のアップグレード](#)が可能になり、[vCenter Server システム、ESXi ホスト、NSX Edge のアップグレード](#)が可能になります。

## vCloud Director インストールの手動アップグレード

1 つのセルをアップグレードする場合は、コマンド オプションを指定せずに vCloud Director インストーラを実行します。アップグレードしたセルを再起動する前に、データベース スキーマをアップグレードする必要があります。サーバ グループ内のセルを 1 つでもアップグレードしたら、データベース スキーマをアップグレードします。

Linux 用の vCloud Director インストーラを使用すると、サポート対象 Linux OS 上の vCloud Director インストール環境で構成される vCloud Director サーバ グループをアップグレードできます。vCloud Director サーバ グループが vCloud Director 9.5 アプライアンス環境で構成される場合、Linux 用の vCloud Director インストーラを使用した既存の環境のアップグレードは、移行ワークフローの一環としてのみ可能になります。[13 章 vCloud Director アプライアンスへの移行](#)を参照してください。

複数セルの vCloud Director インストールの場合は、各セルとデータベースを順番に手動でアップグレードする代わりに、vCloud Director インストールの組織的なアップグレードを実行できます。[vCloud Director インストールの組織的なアップグレードの実行](#)を参照してください。

#### 前提条件

- vCloud Director データベース、vSphere コンポーネント、および NSX コンポーネントが新しいバージョンの vCloud Director と互換性があることを確認します。

---

**重要：** 既存の vCloud Director インストールで Oracle データベースまたは Microsoft SQL Server データベースが使用されている場合は、vCloud Director バージョン 10.0 にアップグレードする前に、PostgreSQL データベースに移行したことを確認してください。使用可能なアップグレード パスについては、[12 章 vCloud Director のアップグレード](#)を参照してください。

---

- vCloud Director サーバ グループに属するサーバに対して、スーパー ユーザーの認証情報があることを確認します。
- インストーラにインストール ファイルのデジタル署名を検証させる場合、ターゲット サーバに VMware パブリック キーをダウンロードし、インストールします。インストール ファイルのデジタル署名をすでに検証している場合、インストール中にそれを再び検証する必要はありません。[VMware パブリック キーのダウンロードとインストール](#)を参照してください。
- アップグレード先の vCloud Director ソフトウェアのバージョンを使用するための有効なライセンス キーがあることを確認します。
- すべての ESXi ホストが有効であることを確認します。vCloud Director 9.5 以降では、無効な ESXi ホストはサポートされません。

#### 手順

##### 1 vCloud Director セルのアップグレード

vCloud Director インストーラは、ターゲット サーバがアップグレードの前提条件をすべて満たしていることを確認し、サーバの vCloud Director ソフトウェアをアップグレードします。

##### 2 vCloud Director データベースのアップグレード

アップグレードした vCloud Director サーバで、vCloud Director データベースをアップグレードするツールを実行します。アップグレードした vCloud Director サーバを再起動する前に、必ず共有データベースをアップグレードする必要があります。

#### 次のステップ

- サーバ グループ内のすべての vCloud Director サーバとそのデータベースをアップグレードしたら、すべてのセルで vCloud Director サービスを起動できます。
- [接続済み vCenter Server システムに関連付けられた各 NSX Manager のアップグレード](#)
- 各 NSX Manager をアップグレードした後、vCenter Server のシステム、ホスト、および NSX Edge をアップグレードできます。[vCenter Server システム、ESXi ホスト、NSX Edge のアップグレード](#)を参照してください。

## vCloud Director セルのアップグレード

vCloud Director インストーラは、ターゲット サーバがアップグレードの前提条件をすべて満たしていることを確認し、サーバの vCloud Director ソフトウェアをアップグレードします。

vCloud Director for Linux は、`vmware-vcloud-director-distribution-v` という形式の名前のデジタル署名された実行可能ファイルとして配布されます。`v.v-nnnnnn.bin`。ここで `vv.v` は、製品バージョン、`nnnnnn` はビルド番号を表します。例えば、`vmware-vcloud-director-distribution-8.10.0-3698331.bin` というファイル名になります。この実行可能ファイルを実行すると、vCloud Director がインストールまたはアップグレードされます。

複数セルの vCloud Director インストールの場合は、vCloud Director サーバ グループのメンバーごとに vCloud Director インストーラを実行する必要があります。

### 手順

- 1 ターゲット サーバに root としてログインします。

- 2 インストール ファイルをターゲット サーバにダウンロードします。

メディアでソフトウェアを購入した場合は、ターゲット サーバからアクセス可能な場所にインストール ファイルをコピーします。

- 3 ダウンロード ページに投稿されているものとダウンロードのチェックサムが一致することを確認します。

MD5 と SHA1 チェックサムの値が、ダウンロード ページに投稿されます。適切なツールを使用して、ダウンロードされたインストール ファイルのチェックサムがダウンロード ページのものと一致することを確認します。次の形式の Linux コマンドは `installation-file` のチェックサムを表示します。

```
[root@cell1 /tmp]# md5sum installation-file
```

コマンドはインストール ファイルのチェックサムを返します。これは、ダウンロード ページの MD5 チェックサムと一致する必要があります。

- 4 インストール ファイルが実行可能であることを確認します。

インストール ファイルには実行権限が必要です。この権限を確実にインストール ファイルに設定するには、コンソール、シェル、またはターミナル ウィンドウを開き、次の Linux コマンドを実行します。`installation-file` は、vCloud Director インストール ファイルへのフル パス名です。

```
[root@cell1 /tmp]# chmod u+x installation-file
```

- 5 インストール ファイルを実行します。

インストール ファイルを実行するには、フル パス名を入力します。次に例を示します。

```
[root@cell1 /tmp]# ./installation-file
```

ファイルには、インストール スクリプトと組み込みの RPM パッケージが含まれます。

**注：** パス名に埋め込まれたスペース文字を含むディレクトリからインストール ファイルを実行することはできません。

インストーラは、vCloud Director のバージョンが、インストール ファイル内のバージョン以降のものであることを検出すると、エラー メッセージを表示して終了します。

インストーラが vCloud Director の以前のバージョンを検出した場合、アップグレードを確認するように求められます。

**6 y** と入力し、Enter キーを押して、アップグレードすることを確認します。

インストーラが以下のアップグレード ワークフローを開始します。

- a ホストがすべての要件を満たすことを確認する。
- b vCloud DirectorRPM パッケージを展開する。
- c セル上のすべてのアクティブ vCloud Director ジョブが完了すると、サーバ上で vCloud Director サービスが停止し、インストール済みの vCloud Director ソフトウェアがアップグレードされます。

ターゲット サーバに VMware パブリック キーをインストールしなかった場合、インストーラは次の形式の警告を表示します。

```
warning: installation-file.rpm: Header V3 RSA/SHA1 signature: NOKEY, key ID 66fd4949
```

ターゲット サーバ上の既存の `global.properties` ファイルを変更しようとする、インストーラは次の形式の警告を表示します。

```
warning: /opt/vmware/vcloud-director/etc/global.properties created as /opt/vmware/vcloud-director/etc/global.properties.rpmnew
```

**注：** 既存の `global.properties` ファイルを以前に更新したことがある場合は、その変更内容を `global.properties.rpmnew` から取得できます。

**7** (オプション) ログ記録プロパティを更新します。

アップグレードした後に、新しいログ記録プロパティがファイル `/opt/vmware/vcloud-director/etc/log4j.properties.rpmnew` に書き込まれます。

オプション	アクション
既存のログ記録プロパティを変更しなかった場合	このファイルを <code>/opt/vmware/vcloud-director/etc/log4j.properties</code> にコピーします。
ログ記録プロパティを変更した場合	変更内容を保持するには、 <code>/opt/vmware/vcloud-director/etc/log4j.properties.rpmnew</code> を既存の <code>/opt/vmware/vcloud-director/etc/log4j.properties</code> ファイルにマージします。

**結果**

vCloud Director のアップグレードが完了すると、以前の設定ファイルの場所に関する情報を示すメッセージがインストーラによって表示されます。インストーラに、データベース アップグレード ツールを実行するように求められます。

**次のステップ**

まだアップグレードしていない場合は、vCloud Director データベースをアップグレードできます。



サーバ グループ内の各 vCloud Director セルでこの手順を繰り返します。

**重要：** サーバ グループおよびデータベースのすべてのセルをアップグレードするまで、vCloud Director サービスを起動しないでください。

## vCloud Director データベースのアップグレード

アップグレードした vCloud Director サーバで、vCloud Director データベースをアップグレードするツールを実行します。アップグレードした vCloud Director サーバを再起動する前に、必ず共有データベースをアップグレードする必要があります。

実行中および最近完了したタスクすべてに関する情報は、vCloud Director データベースに保存されます。データベースをアップグレードすると、このタスク情報が無効になります。そのため、データベース アップグレード ユーティリティは、実行中のタスクがないことを確認してから、アップグレード プロセスを開始します。

vCloud Director サーバ グループ内のすべてのセルは、同じデータベースを共有します。アップグレードするセルの数に関係なく、データベースのアップグレードは 1 回だけ実行します。データベースをアップグレードした後、アップグレードされていない vCloud Director セルはデータベースに接続できません。アップグレードされたデータベースに接続するには、すべてのセルをアップグレードする必要があります。

### 前提条件

- 既存のデータベースをバックアップします。データベース ソフトウェア ベンダーが推奨する手順に従います。
- サーバ グループ内のすべての vCloud Director セルが停止していることを確認します。アップグレードされたセルは、アップグレード プロセスの間は停止しています。まだアップグレードされていない vCloud Director サーバがある場合は、セル管理ツールを使用してサービスを停止し、シャットダウンします。セル管理ツールを使用してセルを管理する方法については、『[10 章 セル管理ツール リファレンス](#)』を参照してください。
- [データベース アップグレード ユーティリティ リファレンス](#)のトピックを参照してください。

### 手順

- 1 オプションを指定して、またはオプションなしで、データベース upgrade ユーティリティを実行します。

```
/opt/vmware/vcloud-director/bin/upgrade
```

NSX Manager の互換性のないバージョンがデータベース アップグレード ユーティリティで検出された場合は、警告メッセージが表示され、アップグレードはキャンセルされます。

- 2 コマンド プロンプトに対して **y** と入力し、Enter キーを押して、データベースをアップグレードすることを確認します。
- 3 コマンド プロンプトに対して **y** と入力し、Enter キーを押して、データベースをバックアップすることを確認します。  
  
--backup-completed オプションを使用した場合、このプロンプトはスキップされます。
- 4 アクティブなセルがユーティリティによって検出された場合は、続行を求めるプロンプトに対して **n** と入力してシェルを終了してから、稼働中のセルがないことを確認し、[手順 手順 1](#) からアップグレードを再試行します。



## 結果

データベース アップグレード ツールが実行されて、進行状況を示すメッセージが表示されます。アップグレードが完了したら、現在のサーバで vCloud Director サービスを開始するように求められます。

## 次のステップ

y と入力し、Enter キーを押すか、後から `service vmware-vcd start` コマンドを実行してサービスを開始します。

アップグレードされた vCloud Director サーバのサービスを開始できます。

サーバ グループに属する残りの vCloud Director メンバーをアップグレードし、そのサービスを開始できます。

[vCloud Director セルのアップグレード](#)を参照してください。

# データベース アップグレード ユーティリティ リファレンス

upgrade ユーティリティを実行するときは、コマンド行に設定情報をオプションおよび引数として指定します。

upgrade ユーティリティの場所は `/opt/vmware/vcloud-director/bin/` です。

表 12-1. データベース アップグレード ユーティリティのオプションおよび引数

オプション	引数	説明
<code>--backup-completed</code>	なし	vCloud Director のバックアップが完了していることを指定します。このオプションを指定すると、アップグレード ユーティリティは、データベースをバックアップするかどうかを尋ねるプロンプトを表示しなくなります。
<code>--ceip-user</code>	CEIP サービス アカウントのユーザー名。	このユーザー名のユーザーがすでにシステム組織にすでに含まれている場合は、アップグレードが失敗します。デフォルト: <code>phone-home-system-account</code> 。
<code>--enable-ceip</code>	次のいずれかを選択します <ul style="list-style-type: none"> <li>■ <code>true</code></li> <li>■ <code>false</code></li> </ul>	このインストール環境が VMware カスタム エクスペリエンス改善プログラム (CEIP) に参加するかどうかを指定します。このオプションを省略した場合で、なおかつ現在の構成で <code>false</code> に設定されていないとき、デフォルトは <code>true</code> です。VMware のカスタム エクスペリエンス改善プログラム (CEIP) に参加すると、CEIP を介して収集されたデータに関する追加情報が提供されます。VMware によるこの情報の使用目的は、 <a href="http://www.vmware.com/trustvmware/ceip.html">http://www.vmware.com/trustvmware/ceip.html</a> の Trust & Assurance Center で設定されています。セル管理ツールを使用して、この製品の VMware CEIP への参加または離脱をいつでも実行できます。『 <a href="#">10 章 セル管理ツール リファレンス</a> 』を参照してください。

表 12-1. データベース アップグレード ユーティリティのオプションおよび引数 (続き)

オプション	引数	説明
--installer-path	vCloud Director インストール ファイルのフル パス名。インストール ファイルとそれが格納されているディレクトリは、ユーザー vcloud.vcloud が読み取り可能である必要があります。	--private-key-path オプションが必須です。
--maintenance-cell	IP アドレス	アップグレード時にアップグレード ユーティリティがメンテナンス モードで実行するためのセルの IP アドレス。このセルは、他のセルがシャットダウンする前にメンテナンス モードに入り、他のセルのアップグレード中はメンテナンス モードのままになります。他のセルがアップグレードされ、それらのセルの 1 つ以上が再起動すると、このセルはシャットダウンされ、アップグレードされます。--private-key-path オプションが必須です。
--multisite-user	マルチサイト システムのアカウントのユーザー名。	このアカウントは、vCloud Director マルチサイト機能で使用されます。このユーザー名のユーザーがすでにシステム組織にすでに含まれている場合は、アップグレードが失敗します。デフォルト: multisite-system-account。
--private-key-path	パス名	セルのプライベート キーのフル パス名。このオプションを使用すると、サーバ グループ内のすべてのセルが、データベースのアップグレード後に正常にシャットダウン、アップグレード、および再起動されます。このアップグレード ワークフローの詳細については、 <a href="#">vCloud Director インストールの組織的なアップグレードの実行</a> を参照してください。
--unattended-upgrade	なし	無人アップグレードを指定します

--private-key-path オプションを使用する場合、パスワードを要求せずにスーパーユーザーからの ssh 接続を許可するように、すべてのセルを設定する必要があります。これを確認するには、次に示すような Linux コマンド ラインを使用します。この例では、ID が vcloud に設定され、cell-ip にあるセルへの ssh 接続が root として確立されますが、root パスワードの指定はありません。

```
sudo -u vcloud ssh -i private-key-path root@cell-ip
```

ローカル セルの *private-key-path* にあるプライベート キーがユーザー `vcloud.vcloud` から読み取り可能で、対応するパブリック キーが *cell-ip* の root ユーザーの `authorized-keys` ファイルに追加されていれば、コマンドが成功します。

---

**注：** vCloud Director プロセスを実行する ID として使用するため、vCloud Director インストーラにより、`vcloud` ユーザー、`vcloud` グループ、および `vcloud.vcloud` アカウントが作成されます。`vcloud` ユーザーにはパスワードがありません。

---

# vCloud Director アプライアンスへの移行

# 13

バージョン 9.7 以降、vCloud Director アプライアンスには、高可用性機能を備えた組み込みの PostgreSQL データベースが含まれています。外部 PostgreSQL データベースを使用する、以前のバージョンに基づく既存の vCloud Director 環境を、vCloud Director 10.0 アプライアンス環境で構成されている vCloud Director 環境に移行できます。

Linux 上の vCloud Director インストール環境または vCloud Director アプライアンス環境で構成されている vCloud Director 環境を移行できます。バージョン 10.0 以降では、Microsoft SQL データベースはサポートされなくなり、外部 PostgreSQL データベースを使用する vCloud Director 環境からのみ移行できます。

vCloud Director 環境で外部 Oracle データベースまたは外部 Microsoft SQL データベースを使用している場合は、vCloud Director 10.0 にアップグレードする前に、PostgreSQL データベースに移行する必要があります。アップグレードパスについては、[12 章 vCloud Director のアップグレード](#)を参照してください。

この章には、次のトピックが含まれています。

- [外部 PostgreSQL データベースを使用する vCloud Director の vCloud Director アプライアンスへの移行](#)

## 外部 PostgreSQL データベースを使用する vCloud Director の vCloud Director アプライアンスへの移行

現在の vCloud Director 環境で外部 PostgreSQL データベースを使用している場合は、vCloud Director アプライアンス環境で構成される新しい vCloud Director 環境に移行できます。現在の vCloud Director 環境は、Linux 上の vCloud Director インストール環境または vCloud Director アプライアンス環境から構成することができます。新しい vCloud Director 環境では、高可用性モードのアプライアンス組み込み PostgreSQL データベースを使用できます。

移行ワークフローには、4 つの主要なステージがあります。

- 既存の vCloud Director 環境をアップグレードする
- vCloud Director アプライアンスのインスタンスを 1 つ以上展開して、新しい vCloud Director サーバグループを作成する
- 外部データベースを組み込みデータベースに移行する
- 共有転送サービスのデータおよび証明書データをコピーする

## 手順

- 1 現在の外部 PostgreSQL データベースのバージョンが 9.x である場合は、外部 PostgreSQL データベースをバージョン 10 以降にアップグレードします。

- 2 現在の vCloud Director 環境をバージョン 10.0 にアップグレードします。

[12 章 vCloud Director のアップグレード](#)を参照してください。

- 3 移行元の vCloud Director の再起動に成功したことを確認します。
- 4 アップグレードされた vCloud Director 環境の各セルで以下のコマンドを実行して、vCloud Director サービスを停止します。

```
/opt/vmware/vcloud-director/bin/cell-management-tool -u <admin username> cell --shutdown
```

- 5 外部 PostgreSQL データベースで、現在のデータベースをバックアップします。

```
sudo -u postgres path_to_pg_dump -Fc db_name > /tmp/db_dump_name
```

/tmp フォルダに十分な空き容量がない場合は、別の場所を使用してダンプ ファイルを保存します。

- 6 データベース所有者とデータベース名が vcloud と異なる場合は、ユーザー名とデータベース名を書き留めておきます。

新しい環境内でこのユーザーを作成し、手順 13 でデータベースの名前を変更する必要があります。

- 7 新しい vCloud Director 環境で既存の環境の IP アドレスを使用する場合は、プロパティと証明書ファイルを外部 PostgreSQL データベース上の場所にコピーして、セルをパワーオフする必要があります。

- a /opt/vmware/vcloud-director/etc/ にある global.properties、responses.properties、certificates、proxycertificates、および truststore ファイルを外部 PostgreSQL データベースの /tmp または推奨場所にコピーします。

- b 既存の環境のセルをパワーオフします。

- 8 新しい vCloud Director 環境で既存の環境の NFS サーバを使用する場合は、この NFS サーバ上に、新しい共有 NFS マウントポイントとしてディレクトリを新規作成し、エクスポートします。

古い NFS のユーザー ID およびグループ ID (UID/GID) は新しい NFS のユーザー ID およびグループ ID と一致しない可能性があるため、既存のマウントポイントを再利用することはできません。

- 9 vCloud Director 10.0 アプライアンスのインスタンスを 1 つ以上デプロイして、新しいサーバ グループを作成します。

- データベースの高可用性機能を使用する場合は、1 つのプライマリ セルと 2 つのスタンバイ セルをデプロイし、必要に応じて 1 つ以上の vCD アプリケーション セルをデプロイします。
- 既存の環境のセルをパワーオフした場合は、新しいセルに元の IP アドレスを使用できます。
- 既存の NFS サーバに新しいパスをエクスポートした場合は、新しい環境で新しい共有マウントポイントを使用できます。

[6 章 vCloud Director アプライアンスのデプロイ](#)を参照してください。

- 10 新しくデプロイした各セルで以下のコマンドを実行し、vCloud Director サービスを停止します。

```
service vmware-vcd stop
```

- 11 外部 PostgreSQL データベースの /tmp フォルダから、新しい環境のプライマリ セルにある /tmp フォルダにダンプ ファイルをコピーします。

手順 5 を参照してください。

- 12 ダンプ ファイルの権限を変更します。

```
chmod a+r /tmp/db_dump_name
```

- 13 新しくデプロイされたプライマリ セルのコンソールに root としてログインし、外部データベースから組み込みデータベースに vCloud Director データベースを転送します。

- a ユーザーを postgres に切り替えて psql データベース ターミナルに接続し、次のステートメントを実行して vcloud データベースを削除します。

```
sudo -i -u postgres /opt/vmware/vpostgres/current/bin/psql -c 'DROP DATABASE vcloud;'
```

- b 既存の外部データベースのデータベース所有者が vcloud と異なる場合は、手順 6 で書き留めた名前のユーザーを作成します。

```
sudo -i -u postgres /opt/vmware/vpostgres/current/bin/psql -c 'CREATE USER  
<db_owner_external_pg>;'
```

- c pg\_restore コマンドを実行します。

```
sudo -u postgres /opt/vmware/vpostgres/current/bin/pg_restore -C -d postgres /tmp/db_dump_name
```

- d 既存の外部データベースのデータベース名が vcloud と異なる場合は、手順 6 で書き留めた名前を使用してデータベース名を vcloud に変更します。

```
sudo -i -u postgres /opt/vmware/vpostgres/current/bin/psql -c 'ALTER DATABASE  
<db_name_external_pg> RENAME TO vcloud;'
```

- e 既存の vCloud Director 環境のデータベース所有者が vcloud と異なる場合は、データベース所有者を vcloud に変更して、テーブルを vcloud に再割り当てします。

```
sudo -i -u postgres /opt/vmware/vpostgres/current/bin/psql -c 'ALTER DATABASE vcloud OWNER TO  
vcloud;'
```

```
sudo -i -u postgres /opt/vmware/vpostgres/current/bin/psql -d vcloud -c 'REASSIGN OWNED BY  
<db_owner_external_pg> TO vcloud;'
```

- 14 新しくデプロイされた各セルで、構成データのバックアップと置き換えを行い、vCloud Director サービスを再構成して開始します。

- a プロパティ、トラストストア、証明書ファイルをバックアップし、移行元の外部 PostgreSQL データベース上の場所（手順 7a でファイルをコピーした場所）からこれらのファイルをコピーして、置き換えます。

global.properties、responses.properties、truststore、certificates、および proxycertificates ファイルは /opt/vmware/vcloud-director/etc/ にあります。

- b /opt/vmware/vcloud-director/certificates.ks にあるキーストア ファイルをバックアップします。

移行元からキーストア ファイルをコピーして置き換えないようにしてください。

- c 以下のコマンドを実行して、vCloud Director サービスを再構成します。

```
/opt/vmware/vcloud-director/bin/configure --unattended-installation --database-type postgres
--database-user vcloud \
--database-password db_password_new_primary --database-host eth1_ip_new_primary --database-
port 5432 \
--database-name vcloud --database-ssl true --uuid --keystore /opt/vmware/vcloud-director/
certificates.ks \
--keystore-password root_password_new_primary --primary-ip appliance_eth0_ip \
--console-proxy-ip appliance_eth0_ip --console-proxy-port-https 8443
```

各値は次のとおりです。

- --keystore-password の値は、このアプライアンスの初期 root パスワードと一致します。
- --database-password の値は、アプライアンスのデプロイ時に設定したデータベースのパスワードと一致します。
- --database-host の値は、プライマリ アプライアンスの eth1 ネットワーク IP アドレスと一致します。
- --primary-ip の値は、アプライアンスの eth0 ネットワーク IP アドレスと一致します。
- --console-proxy-ip の値は、アプライアンスの eth0 ネットワーク IP アドレスと一致します。
- --console-proxy-port の値は、アプライアンス コンソール プロキシ ポート 8443 と一致します。

トラブルシューティングの詳細については、[vCloud Director アプライアンスに移行またはリストアすると vCloud Director サービスの再構成に失敗する](#)を参照してください。

- d 以下のコマンドを実行して、vCloud Director サービスを開始します。

```
service vmware-vcd start
```

セルの起動の進行状況は /opt/vmware/vcloud-director/logs/cell.log で監視できます。

- 15 HTTP、HTTPS、および TCP トラフィックのロードバランサ プールに新しいアプライアンス eth0 のすべての IP アドレスを含めるようにロードバランサの設定を変更し、これらのプールから古い Linux vCloud Director セルの IP アドレスを削除します。
- 16 新しいサーバ グループのすべてのセルの起動プロセスが終了したら、vCloud Director 環境が正常に移行したことを確認します。
  - a 新しいサーバ グループ [https://eth0\\_IP\\_new\\_cell/provider](https://eth0_IP_new_cell/provider) 内の任意のセルの eth0 ネットワーク IP アドレスを使用して、Service Provider Admin Portal を開きます。
  - b 既存のシステム管理者の認証情報を使用して、Service Provider Admin Portal にログインします。

- c 新しい環境で vSphere およびクラウド リソースが使用可能であることを検証します。
- 17 vCloud Director が正常に移行したことを確認したら、Service Provider Admin Portal を使用して、古い vCloud Director 環境に属する切断されたセルを削除します。
- a メイン メニュー (☰) から、[クラウド リソース] を選択します。
  - b 左側のパネルで [クラウド セル] をクリックします。
  - c 無効なセルを選択し、[登録解除] をクリックします。

vCloud Director アプライアンスを展開して、移行済み環境のサーバ グループにメンバーを追加することができます。

## 次の操作

移行された新しい vCloud Director アプライアンス環境では、自己署名証明書が使用されます。古い環境内の適切に署名された証明書を使用するには、新しい環境の各セルで次の手順を実行します。

- 1 古いセルから `/opt/vmware/vcloud-director/data/transfer/certificates.ks` にキーストア ファイルをコピーして置き換えます。
- 2 セル管理ツール コマンドを実行して、証明書を置き換えます。

vcloud.vcloud がこのファイルの所有者であることを確認してください。

```
/opt/vmware/vcloud-director/bin/cell-management-tool certificates -j -p --keystore /opt/vmware/
vcloud-director/data/transfer/certificates.ks \
--keystore-password ks_password_old_vCD
```

- 3 vCloud Director サービスを再起動します。

```
service vmware-vcd restart
```

このサーバ グループに新しいメンバーを追加すると、これらの適切に署名された証明書を使用して新しいアプライアンス セルがデプロイされます。



# vCloud Director をアップグレードまたは移行した後に行う作業

# 14

すべての vCloud Director サーバと共有データベースをアップグレードまたは移行した後、クラウドにネットワーク サービスを提供する NSX Manager インスタンスをアップグレードできます。その後、vCloud Director インストールに登録されている ESXi ホストと vCenter Server インスタンスをアップグレードできます。

**重要：** バージョン 9.7 以降では、vCloud Director でサポートされるのは詳細 Edge Gateway のみです。詳細以外のレガシー Edge Gateway を詳細 Edge Gateway に変換する必要があります。<https://kb.vmware.com/kb/66767> を参照してください。

この章には、次のトピックが含まれています。

- 接続済み vCenter Server システムに関連付けられた各 NSX Manager のアップグレード
- vCenter Server システム、ESXi ホスト、NSX Edge のアップグレード

## 接続済み vCenter Server システムに関連付けられた各 NSX Manager のアップグレード

vCloud Director に登録されている vCenter Server と ESXi ホストをアップグレードする前に、その vCenter Server に関連付けられている各 NSX Manager をアップグレードする必要があります。

NSX Manager のアップグレード中、NSX 管理機能へのアクセスは中断されますが、ネットワーク サービスは中断されません。NSX Manager のアップグレードは、vCloud Director セルが実行中であるかどうかにかかわらず、vCloud Director のアップグレードの前または後に実行できます。

NSX をアップグレードする方法については、NSX for vSphere のドキュメント (<https://docs.vmware.com>) を参照してください。

### 手順

- 1 vCloud Director インストール環境に登録されている各 vCenter Server に関連付けられた NSX Manager をアップグレードします。
- 2 すべての NSX Manager をアップグレードしたら、登録済みの vCenter Server システムと ESXi ホストをアップグレードできます。

# vCenter Server システム、ESXi ホスト、NSX Edge のアップグレード

vCloud Director および NSX Manager のアップグレードが終わったら、vCloud Director に登録されている vCenter Server システムおよび ESXi ホストをアップグレードする必要があります。接続されているすべての vCenter Server システムおよび ESXi ホストのアップグレードが終わると、NSX Edge をアップグレードすることができます。

## 前提条件

クラウドに接続済みの vCenter Server システムに関連付けられた各 NSX Manager がすでにアップグレードされていることを確認します。[接続済み vCenter Server システムに関連付けられた各 NSX Manager のアップグレード](#)を参照してください。

## 手順

### 1 vCenter Server インスタンスを無効にします。

- vCloud Director Service Provider Admin Portal のメイン メニュー (≡) から、[vSphere リソース] を選択します。
- 左側のパネルで [vCenter] をクリックします。
- 無効にする vCenter Server の横にあるラジオ ボタンを選択して、[無効化] をクリックします。
- [OK] をクリックします。

### 2 vCenter Server システムをアップグレードします。

詳細については、vCenter Server のアップグレードに関する説明を参照してください。

### 3 すべての vCloud Director パブリック URL および証明書チェーンを確認します。

- メイン メニュー (≡) から、[管理] を選択します。
- 左側のパネルの [設定] で、[公開アドレス] をクリックします。
- すべてのパブリック アドレスを確認します。

### 4 vCenter Server の登録を vCloud Director で更新します。

- vCloud Director Service Provider Admin Portal のメイン メニュー (≡) から、[vSphere リソース] を選択します。
- 左側のパネルで [vCenter] をクリックします。
- ターゲット vCenter Server の横にあるラジオ ボタンを選択し、[再接続] をクリックします。
- [OK] をクリックします。

## 5 アップグレードされた vCenter Server システムがサポートする各 ESXi ホストをアップグレードします。

『VMware ESXi のアップグレード』を参照してください。

**重要：** アップグレードされたホストに、クラウドの仮想マシンをサポートするための十分な容量を確保するために、小さなバッチに分けてホストをアップグレードしてください。これを行うとき、ホスト エージェントのアップグレードは、仮想マシンがアップグレードされたホストに移行して戻せるように、時間内に完了することができます。

- a vCenter Server システムを使用して、ホストをメンテナンス モードにし、このホストのすべての仮想マシンを別のホストに移行できるようにします。
- b ホストをアップグレードします。
- c vCenter Server システムを使用してホストを再接続します。
- d vCenter Server システムを使用してホストのメンテナンス モードを終了します。

## 6 (オプション) アップグレード後の vCenter Server システムに関連付けられている NSX Manager が管理する NSX Edge をアップグレードします。

アップグレードされた NSX Edge では、パフォーマンスや連携が向上しています。NSX Manager または vCloud Director を使用して NSX Edge をアップグレードできます。

- NSX Manager を使用して NSX Edge をアップグレードする方法については、NSX for vSphere のドキュメント (<https://docs.vmware.com>) を参照してください。
- vCloud Director を使用して NSX Edge Gateway をアップグレードする場合は、その Edge によってサポートされている vCloud Director ネットワーク オブジェクトを対象に操作する必要があります。
  - vCloud Director または vCloud API のいずれかを使用して Edge Gateway サーバによって提供されるネットワークをリセットすると、Edge Gateway の適切なアップグレードが自動的に実行されます。
  - Edge ゲートウェイを再デプロイすると、関連付けられた NSX Edge アプライアンスがアップグレードされます。

**注：** 再デプロイがサポートされるのは、NSX Data Center for vSphere Edge Gateway のみです。

- vApp アップグレードのコンテキスト内から vApp ネットワークをリセットすると、そのネットワークに関連付けられた NSX Edge アプライアンスがアップグレードされます。vApp のコンテキスト内から vApp ネットワークをリセットするには、vApp の [ネットワーク] タブに移動して、そのネットワークの詳細を表示し、vApp ネットワークの名前の横にあるラジオ ボタンをクリックして、[リセット] をクリックします。

Edge Gateway を再デプロイする方法および vApp ネットワークをリセットする方法の詳細については、『vCloud API プログラミング ガイド』を参照してください。

### 次のステップ

この手順を、vCloud Director インストール環境に登録された他の vCenter Server システムについて繰り返します。

# vCloud Director ログの表示

# 15

vCloud Director では、システムのクラウド セルごとにログ情報を提供します。ログを表示して、セルの監視や問題のトラブルシューティングを行うことができます。

セルのログは `/opt/vmware/vcloud-director/logs` にあります。表 15-1. vCloud Director のログでは、使用可能なログを一覧表示しています。

表 15-1. vCloud Director のログ

ログ名	説明
cell.log	vCloud Director セルからのコンソール出力。
cell-management-tool	セルからのセル管理ツール ログ メッセージ。
cell-runtime	セルからのランタイム ログ メッセージ。
cloud-proxy	セルからのクラウド プロキシ ログ メッセージ。
console-proxy	セルからのリモート コンソール プロキシ ログ メッセージ。
server-group-communications	セルからのサーバ グループ通信。
statsfeeder	vCenter Server からの仮想マシン メトリックの取得、およびストレージ情報とエラー メッセージ。
vcloud-container-debug.log	セルからのデバッグ レベルのログ メッセージ。
vcloud-container-info.log	セルからの情報ログ メッセージ。このログには、セルで発生した警告とエラーも表示されます。
vmware-vcd-watchdog.log	セル ウォッチドッグからの情報ログ メッセージ。セルがいつクラッシュしたか、再起動したかなどが記録されます。
diagnostics.log	セル診断ログ。このファイルは、ローカル ログ構成で診断ログが有効になっていない場合は空です。
YYYY_MM_DD.request.log	Apache 共通ログ形式の HTTP 要求ログ。

ログは、任意のテキスト エディタ/ビューアまたはサードパーティ ツールを使用して表示できます。

# vCloud Director アプライアンスのトラブルシューティング

# 16

vCloud Director アプライアンスのデプロイに失敗した場合、またはアプライアンスが正常に動作していない場合は、アプライアンスのログ ファイルを調べて問題の原因を特定できます。

VMware テクニカル サポートは、定期的に診断情報を要求してサポート リクエストを処理します。vmware-vcd-support スクリプトを使用して、ホスト ログ情報および vCloud Director ログを収集できます。vCloud Director の診断情報の収集の詳細については、<https://kb.vmware.com/s/article/1026312> を参照してください。vmware-vcd-support スクリプトを実行すると、廃止または置き換えられたセルに関する情報が FAIL というステータスでログに含まれることがあります。『<https://kb.vmware.com/s/article/71349>』を参照してください。

この章には、次のトピックが含まれています。

- [vCloud Director アプライアンスのログ ファイルの調査](#)
- [アプライアンスのデプロイ後に vCloud Director のセルの起動に失敗する](#)
- [vCloud Director アプライアンスに移行またはリストアすると vCloud Director サービスの再構成に失敗する](#)
- [ログ ファイルを使用した vCloud Director のアップデートおよびパッチのトラブルシューティング](#)
- [vCloud Director のアップデートの確認に失敗する](#)
- [vCloud Director の最新アップデートのインストールに失敗する](#)

## vCloud Director アプライアンスのログ ファイルの調査

vCloud Director アプライアンスをデプロイした後、firstboot ログおよびデータベース ログでエラーと警告を調べることができます。

### 手順

- 1 vCloud Director アプライアンス コンソールに root として直接ログインするか、SSH で接続します。
- 2 /opt/vmware/var/log に移動します。
- 3 ログ ファイルを調べます。
  - firstboot ファイルには、アプライアンスの最初の起動に関連するログ情報が含まれています。
  - /opt/vmware/var/log/vcd/ ディレクトリには、Replication Manager (repmgr) ツールスイートの設定と再設定、およびアプライアンスの同期に関連するログが含まれています。

- `/opt/vmware/var/log/vcd/pg/` ディレクトリには、組み込みアプライアンス データベースのバックアップに関連するログが含まれています。
- `/opt/vmware/etc/vami/ovfEnv.xml` ファイルには、OVF 展開パラメータが含まれています。

## アプライアンスのデプロイ後に vCloud Director のセルの起動に失敗する

vCloud Director アプライアンスが正常にデプロイされても、vCloud Director サービスの起動に失敗することがあります。

### 問題

アプライアンスのデプロイ後、`vmware-vcd` サービスは非アクティブになります。

### 原因

プライマリ セルをデプロイした場合、NFS 共有転送サービスのストレージが事前入力されているため、vCloud Director サービスの起動に失敗することがあります。プライマリ アプライアンスをデプロイする前に、共有転送サービスのストレージに `responses.properties` ファイルまたは `appliance-nodes` ディレクトリを格納しないでください。

スタンバイ セルまたは vCD アプリケーション セルをデプロイした場合、NFS 共有転送ストレージ内に `responses.properties` ファイルがないため、vCloud Director サービスを起動できないことがあります。スタンバイ アプライアンスまたは vCD アプリケーション アプライアンスをデプロイする前に、共有転送サービスのストレージに `responses.properties` ファイルを格納しておく必要があります。

### 解決方法

- 1 vCloud Director アプライアンス コンソールに `root` として直接ログインするか、SSH で接続します。
- 2 `/opt/vmware/var/log/vcd/setupvcd.log` で NFS ストレージに関するエラー メッセージを調べます。
- 3 アプライアンス タイプに合わせて NFS ストレージを準備します。
- 4 セルを再デプロイします。

## vCloud Director アプライアンスに移行またはリストアすると vCloud Director サービスの再構成に失敗する

vCloud Director アプライアンスへの移行またはリストア時に、`configure` コマンドの実行に失敗することがあります。

### 問題

vCloud Director を新しい vCloud Director アプライアンス環境に移行またはリストアする手順では、`configure` コマンドを実行して、新しい各セルで vCloud Director サービスを再構成します。`configure` コマンドは、「`sun.security.validator.ValidatorException: PKIX path validation failed: java.security.cert.CertPathValidatorException: signature check failed`」というエラー メッセージと共に失敗することがあります。

### 解決方法

- 1 ターゲット セルで、コマンドを実行します。

```
sed -i '/vcd_ova.crt/ s/$/ --force /' /opt/vmware/appliance/bin/appliance-sync.sh
```

- 2 1 分間待機してから、configure コマンドを再実行します。

## ログ ファイルを使用した vCloud Director のアップデートおよびパッチのトラブルシューティング

パッチを vCloud Director アプライアンスに適用するときに、ログ ファイルにエラーおよび警告がないか調べることができます。

### 問題

vamicli コマンドがエラーを返した場合は、ログ ファイルを使用してのトラブルシューティングを行うことができます。

### 解決方法

- 1 vCloud Director アプライアンス コンソールに root として直接ログインするか、SSH で接続します。
- 2 該当するログ ファイルに移動します。
  - vamicli update --check が失敗した場合は、/opt/vmware/var/log/vami/vami.log に移動します。
  - vamicli update --install latest が失敗した場合は、/opt/vmware/var/log/vami/updatecli.log に移動します。
- 3 ログ ファイルを調べます。

## vCloud Director のアップデートの確認に失敗する

vCloud Director アプライアンスのアップデートを確認するときに、vamicli update --check コマンドの実行に失敗することがあります。

### 問題

パッチを vCloud Director アプライアンスに適用する手順を実行中に、vamicli update --check コマンドを実行して使用可能なアップデートを検索すると、vamicli update --check コマンドが失敗して、「エラー: マニフェストのダウンロード中にエラーが発生しました。ベンダーにお問い合わせください。」というエラーが表示されます。

### 原因

アップデート リポジトリのディレクトリのパスが正しくありません。

## 解決方法

- 1 正しいパスを指定して `vamicli` コマンドを実行します。

```
vamicli update --repo file:/root/local-update-repo
```

- 2 コマンドを再実行して、アップデートを確認します。

```
vamicli update --check
```

## vCloud Director の最新アップデートのインストールに失敗する

vCloud Director アプライアンスに最新のアップデートをインストールするときに、`vamicli update --install latest` コマンドの実行に失敗することがあります。

### 問題

パッチを vCloud Director アプライアンスに適用する手順を実行中に、`vamicli update --install latest` コマンドを実行して使用可能な最新のパッチを適用します。`vamicli update --install latest` コマンドが失敗し、「エラー: パッケージのインストール中にエラーが発生しました」というメッセージが表示されることがあります。

### 原因

このエラーは、NFS サーバにアクセスできない場合に発生します。

### 解決方法

- 1 `/opt/vmware/vcloud-director/data/transfer` にマウントされている NFS サーバにアクセスできることを確認します。
- 2 コマンドを再実行して、使用可能なパッチを適用します。

```
vamicli update --install latest
```



# vCloud Director ソフトウェアのアンインストール

# 17

個々のサーバーから vCloud Director ソフトウェアをアンインストールするには、Linux の rpm コマンドを使用します。

## 手順

- 1 ターゲット サーバに root としてログインします。
- 2 転送サービス ストレージをアンマウントします。通常は、`/opt/vmware/vcloud-director/data/transfer` にマウントされています。
- 3 コンソール、シェル、またはターミナル ウィンドウを開き、Linux rpm コマンドを実行します。

```
rpm -e vmware-pherehome vmware-vcloud-director vmware-vcloud-director-rhel
```

他のインストール パッケージが `vmware-vcloud-director` パッケージに依存している場合は、vCloud Director をアンインストールする前にそれらの依存パッケージをアンインストールするよう求めるプロンプトが表示されます。