

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

変更日：2021 年 8 月 4 日

VMware Cloud Director 10.2

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

ヴィエムウェア株式会社
〒108-0023 東京都港区芝浦 3-1-1
田町ステーションタワー N 18 階
www.vmware.com/jp

Copyright © 2010-2021 VMware, Inc. All rights reserved. 著作権および商標情報。

目次

VMware Cloud Director™ インストール、構成、およびアップグレード ガイド 7

1 VMware Cloud Director のアーキテクチャ 8

2 VMware Cloud Director のハードウェアおよびソフトウェア要件 11

VMware Cloud 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

3 VMware Cloud Director アプライアンスのデプロイ、アップグレード、および管理 15

アプライアンス環境とデータベースの高可用性構成 15

VMware Cloud Director アプライアンスの自動フェイルオーバー 18

障害のあるプライマリ セルの自動フェンス 20

VMware Cloud Director アプライアンスのデプロイの準備 20

VMware Cloud Director アプライアンス用の転送サーバ ストレージの準備 21

VMware Cloud Director 用 NSX Data Center for vSphere のインストールと構成 23

VMware Cloud Director 用 NSX-T Data Center のインストールと構成 24

VMware Cloud Director アプライアンスのデプロイと初期構成 25

VMware Cloud Director アプライアンスのサイジング ガイドライン 27

VMware Cloud Director アプライアンスのデプロイの前提条件 32

vSphere Client を使用した VMware Cloud Director アプライアンスのデプロイ 32

VMware OVF Tool を使用した VMware Cloud Director アプライアンスのデプロイ 39

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 VMware Cloud Director アプライアンスのデプロイ 47

VMware Cloud 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 49

プライベート キーおよび CA 署名付き SSL 証明書の VMware Cloud Director アプライアンスへのインポート 53

VMware Cloud Director アプライアンスのデプロイ後の作業 54

VMware Cloud Director アプライアンスの root パスワードの変更 60

VMware Cloud Director アプライアンスのアップグレードと移行 61

アップデート パッケージを使用した VMware Cloud Director アプライアンスのアップグレード 64

VMware Update Repository を使用した VMware Cloud Director アプライアンスのアップグレード 67

アップグレードが失敗した場合の VMware Cloud Director アプライアンスのロールバック 69

外部 PostgreSQL データベースを使用した VMware Cloud Director の VMware Cloud Director アプライアンスへの移行 70

VMware Cloud Director のアップグレード後 75

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 75

vCenter Server システム、ESXi ホスト、NSX Edge のアップグレード 76

VMware Cloud Director アプライアンスの管理 78

VMware Cloud 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
VMware Cloud Director アプライアンスのフェイルオーバー モードの変更	85
VMware Cloud Director データベースへの外部アクセスの設定	86
VMware Cloud 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	86
VMware Cloud Director アプライアンスでの FIPS モードの有効化または無効化	87
VMware Cloud Director アプライアンス SNMP エージェントの構成	90
VMware Cloud Director アプライアンスの DNS 設定の編集	96
VMware Cloud 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	97
VMware Cloud Director アプライアンスでのスクリプトの設定	98
VMware Cloud Director アプライアンス証明書の更新	98
自己署名の組み込み PostgreSQL および VMware Cloud 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	100
VMware Cloud Director アプライアンス用の転送サーバ ストレージの置き換え	101
VMware Cloud 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	103
VMware Cloud Director アプライアンスでの PostgreSQL 設定の変更	104
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	105
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	105
MQTT クライアントを使用したイベント、タスク、およびメトリックへのサブスクライブ	107
自動スケール グループ	108
VMware Cloud Director アプライアンス データベース クラスタの健全性の監視	110
VMware Cloud Director アプライアンス クラスタの健全性とフェイルオーバー モードの表示	110
VMware Cloud Director アプライアンス サービス ステータスの表示	112
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	113
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	114
VMware Cloud Director サービスのステータスの確認	115
VMware Cloud Director アプライアンス データベース クラスタのリカバリ	116
高可用性クラスタのプライマリ セル障害からのリカバリ	117
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	120
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 セルまたはスタンバイ セルの登録解除	121
アプライアンスのトラブルシューティング	121
VMware Cloud Director アプライアンスのログ ファイルの調査	121
アプライアンスのデプロイ後に VMware Cloud Director のセルの起動に失敗する	122
アプライアンスの初期構成中に NFS 検証が失敗した後のリカバリ	123
VMware Cloud Director アプライアンスに移行またはリストアすると VMware Cloud Director サービスの再構成に失敗する	126
VMware Cloud Director アプライアンスのスタンバイ ノードがアクセス不能になる	127
VMware Cloud Director アプライアンスのスタンバイ ノードが接続解除される	129
クラスタの健全性で SSH の問題が示されている場合	131
ログ ファイルを使用した VMware Cloud 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	135
VMware Cloud Director のアップデートの確認に失敗する	136
VMware Cloud Director の最新アップデートのインストールに失敗する	136

4 Linux での VMware Cloud Director のインストール、アップグレード、および管理 138

構成の計画 138

VMware Cloud Director インストールの準備 139

Linux での VMware Cloud Director の外部 PostgreSQL データベースの構成 139

Linux での VMware Cloud Director の転送サーバストレージの準備 140

VMware パブリック キーのダウンロードとインストール 142

VMware Cloud Director 用 NSX Data Center for vSphere のインストールと構成 143

VMware Cloud Director 用 NSX-T Data Center のインストールと構成 144

Linux への VMware Cloud Director のインストール 145

サーバ グループの後続のメンバーへの VMware Cloud Director のインストール 147

Linux 上の VMware Cloud Director 向けの SSL 証明書の作成と管理 149

ネットワークおよびデータベース接続の構成 155

サーバ グループの後続のメンバーへの VMware Cloud Director のインストール 162

VMware Cloud Director のインストール後 164

Linux での VMware Cloud Director 用パブリック アドレスのカスタマイズ 164

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 166

外部 PostgreSQL データベースでの追加設定の実行 167

RabbitMQ AMQP ブローカのインストールおよび構成 169

MQTT クライアントを使用したイベント、タスク、およびメトリックへのサブスクライブ 170

自動スケール グループ 171

Linux での VMware Cloud Director のアップグレード 173

VMware Cloud Director インストールの組織的なアップグレードの実行 175

VMware Cloud Director インストールの手動アップグレード 178

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 183

VMware Cloud Director のアップグレード後 185

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 186

vCenter Server システム、ESXi ホスト、NSX Edge のアップグレード 186

5 セル管理ツール リファレンス 189

VMware Cloud Director インストール環境の構成 192

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 194

セルの管理 195

セル アプリケーションの管理 197

データベース接続プロパティを更新する 198

破損したスケジューラ データの検出および修復 201

HTTPS 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 202

HTTPS 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 204

外部サービスからの SSL 証明書のインポート 205

vSphere リソースからのエンドポイント証明書のインポート 206

テスト接続拒否リストの構成 207

すべてのアクティブ セルの FIPS ステータスの表示 208

許可された SSL 暗号のリストの管理	209
許可された SSL プロトコルのリストの管理	212
メトリックの収集と公開の構成	214
Cassandra メトリック データベースの構成	217
システム管理者のパスワードの復元	218
タスクの失敗ステータスの更新	219
監査メッセージ処理の構成	220
メール テンプレートの構成	222
親なしの仮想マシンの検索	225
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	227
アプリケーションの設定の更新	228
カタログ同期のスロットリングの設定	228
VMware Cloud 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	229
vCenter Server 仮想マシン検出のデバッグ	230
マルチサイト拡張ネットワークの MAC アドレスの再生成	232
VMware Cloud Director セルのデータベース IP アドレスの更新	233

6 VMware Cloud Director ログの収集 236

7 VMware Cloud Director ソフトウェアのアンインストール 238

VMware Cloud Director™ インストール、構成、およびアップグレード ガイド

VMware Cloud Director インストール、構成、およびアップグレード ガイド は、VMware Cloud Director™ 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®、VMware NSX® for vSphere®、および VMware NSX-T™ 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

『VMware Cloud Director インストール、構成、およびアップグレード ガイド』は、VMware Cloud 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。

VMware Cloud Director のアーキテクチャ

1

VMware Cloud Director サーバ グループは、Linux または VMware Cloud 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 VMware Cloud Director サーバで構成されます。グループの各サーバは VMware Cloud 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 VMware Cloud 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 VMware Cloud Director インストールおよび VMware Cloud 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。

VMware Cloud 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 VMware Cloud 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。

VMware Cloud Director インストールは、複数の VMware vCenter Server[®] 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[™] 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、VMware Cloud 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、VMware Cloud 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. VMware Cloud Director Linux インストールのアーキテクチャ図

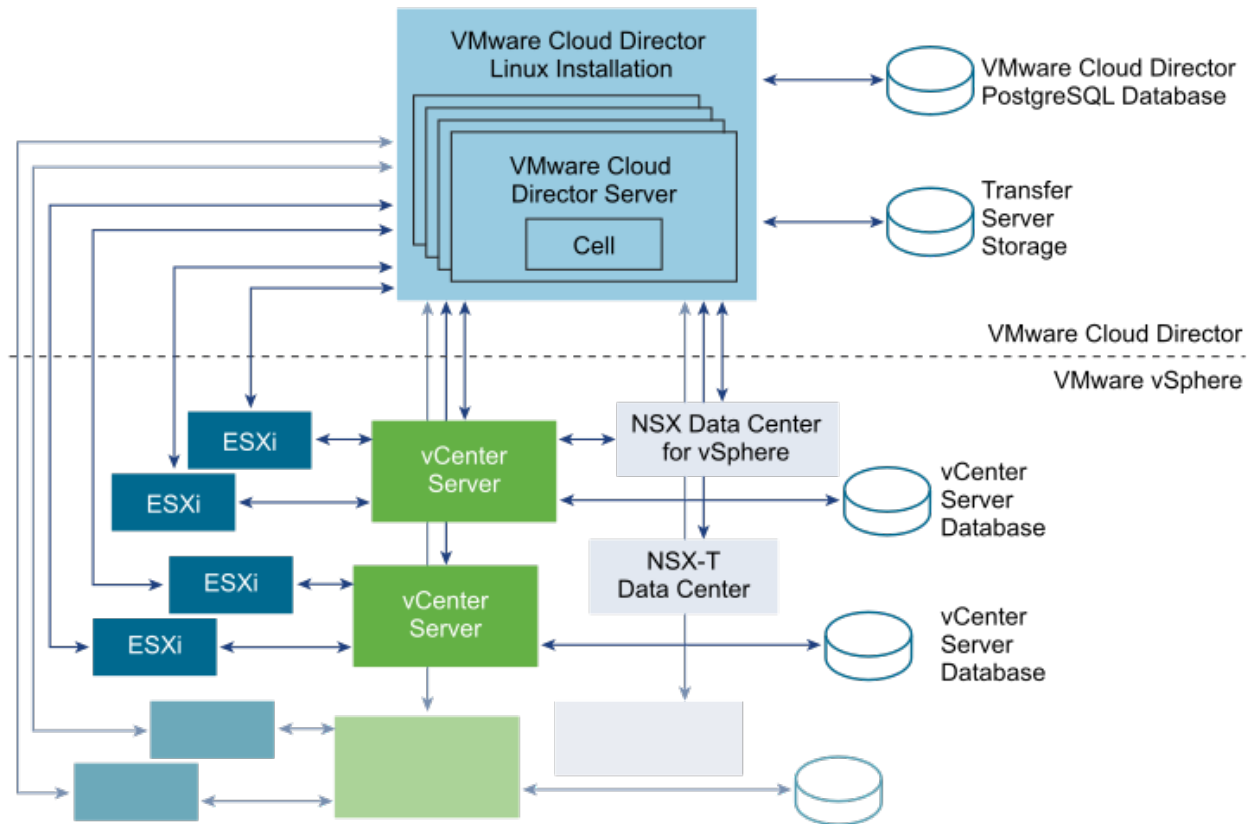
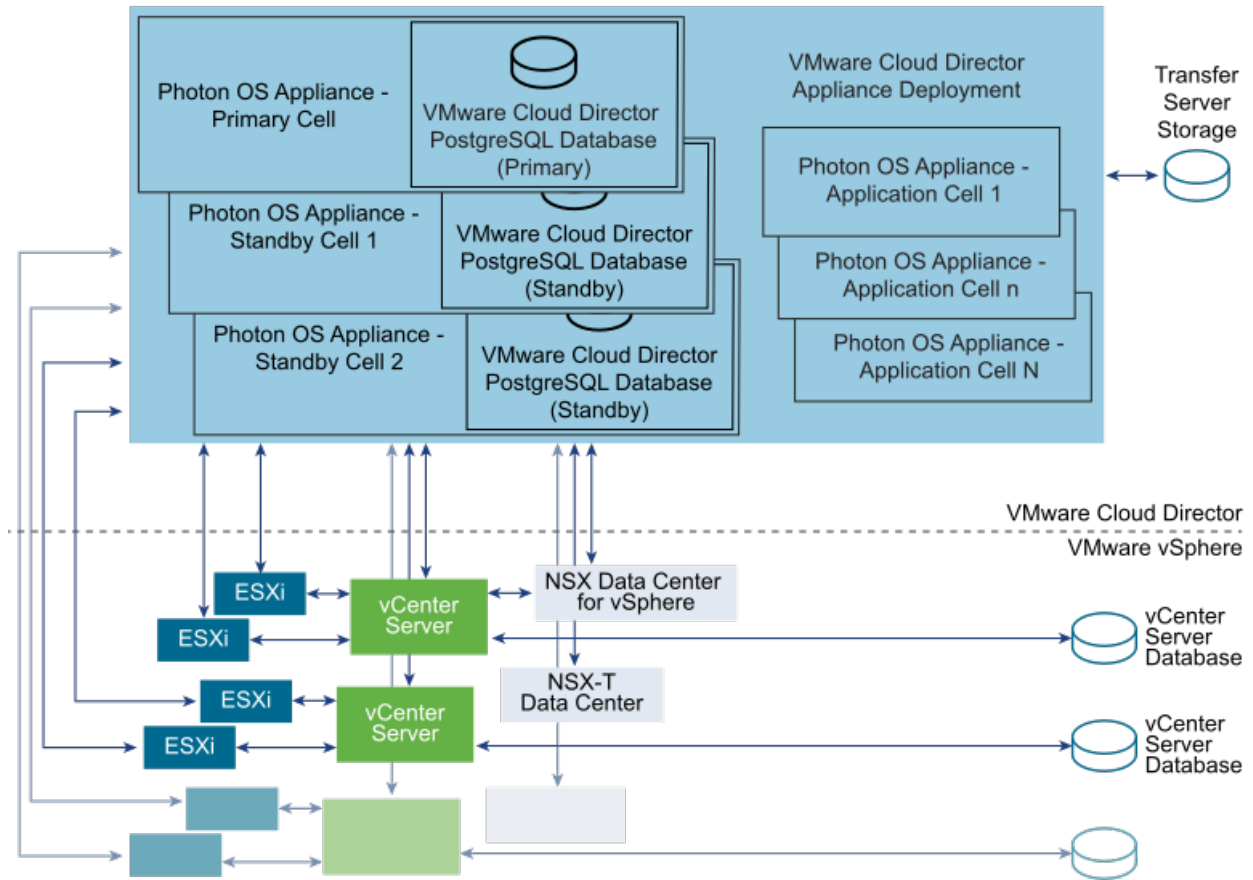


図 1-2. VMware Cloud Director アプライアンスのアーキテクチャ図



Linux にインストールされた VMware Cloud 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 VMware Cloud 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、VMware Cloud 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 1-3. 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 VMware Cloud Director アプライアンス

VMware Cloud 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、『VMware Cloud Director Service Provider Admin Portal Guide』を参照してください。

VMware Cloud Director のハードウェアおよびソフトウェア要件

2

VMware Cloud 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

VMware Cloud 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 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

VMware Cloud 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。

- VMware Cloud 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、VMware Cloud 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 VMware Cloud 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。
- VMware Cloud 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。VMware Cloud 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 およびホスト管理』ドキュメントの「SSL 設定の構成」を参照してください。

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 VMware Cloud 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、『VMware Cloud Director 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、および CPU の要件の詳細については、[VMware Cloud Director アプライアンスのサイジング ガイドライン](#)を参照してください。

共有ストレージ

NFS またはその他の VMware Cloud 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。

- [VMware Cloud 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](#)

VMware Cloud Director のネットワーク構成要件

VMware Cloud 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。VMware Cloud 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。

VMware Cloud 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 VMware Cloud 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、HTTPS 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。

VMware Cloud 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、VMware Cloud 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 サーバを含むすべての VMware Cloud Director サーバのクロックを同期させる必要があります。同期されるサーバのクロック間で許容されるずれは最大 2 秒です。

VMware Cloud Director アプライアンスのデプロイの場合、転送共有に使用される NFS サーバは、NTP などのネットワーク タイムサービスを使用してクロックを VMware Cloud Director アプライアンスのクロックと同期する必要があります。同期されるサーバのクロック間で許容されるずれは最大 2 秒です。

サーバのタイムゾーン

転送共有に使用される NFS サーバやデータベース サーバを含むすべての VMware Cloud Director サーバは、同じタイムゾーンになるように設定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、VMware Cloud 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

VMware Cloud 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、VMware Cloud 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 VMware Cloud Director サーバを、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。

VMware Cloud Director で使用されるネットワーク ポートおよびプロトコルの詳細については、「[VMware Ports and Protocols](#)」を参照してください。

VMware Cloud 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。

- VMware Cloud Director を公開インターネットに直接接続しないでください。VMware Cloud 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。

VMware Cloud Director ホストからの受信パケットを許可する必要があるポートの詳細については、[VMware Ports and Protocols](#) を参照してください。

- 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。

VMware Cloud Director ホストからの送信パケットを許可する必要があるポートの詳細については、[VMware Ports and Protocols](#) を参照してください。

- バージョン 10.1 以降では、サービス プロバイダとテナントは VMware Cloud Director API を使用してリモート サーバへの接続をテストし、サーバ ID を SSL ハンドシェイクの一部として検証できます。VMware Cloud Director ネットワーク接続を保護するために、VMware Cloud Director API を使用して接続テストを行っているテナントからは到達できない内部ホストの拒否リストを構成します。VMware Cloud Director をインストールまたはアップグレードしてから、テナントに VMware Cloud Director へのアクセスを許可するまでの間に、拒否リストを構成します。[テスト接続の拒否リストの構成](#)を参照してください。
- 専用のプライベート ネットワーク上で、VMware Cloud 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。
 - VMware Cloud 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、VMware Cloud 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。VMware Cloud 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。

VMware Cloud Director アプライアンスのデプロイ、アップグレード、および管理

3

バージョン 9.7 以降、VMware Cloud 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。VMware Cloud Director アプライアンスをデプロイ、アップグレード、移行するときに、管理、監視、修正、またはトラブルシューティングの操作を実行できます。

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](#)
- [VMware Cloud Director アプライアンスのデプロイの準備](#)
- [VMware Cloud Director アプライアンスのデプロイと初期構成](#)
- [VMware Cloud Director アプライアンスのアップグレードと移行](#)
- [VMware Cloud Director のアップグレード後](#)
- [VMware Cloud Director アプライアンスの管理](#)
- [VMware Cloud Director アプライアンス データベース クラスタの健全性の監視](#)
- [VMware Cloud Director アプライアンス データベース クラスタのリカバリ](#)
- [アプライアンスのトラブルシューティング](#)

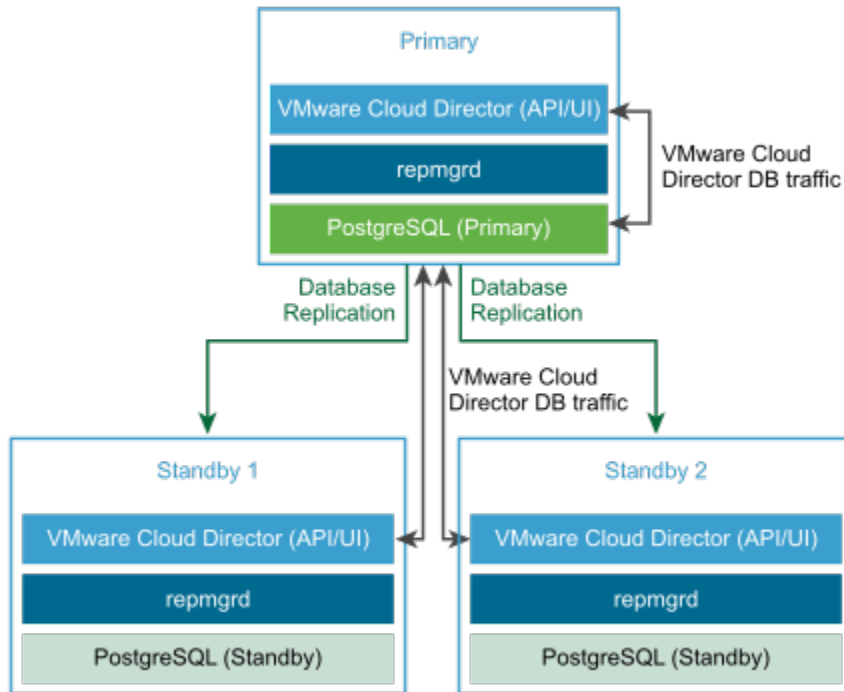
アプライアンス環境とデータベースの高可用性構成

VMware Cloud 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。VMware Cloud 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。

VMware Cloud 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 VMware Cloud Director 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 VMware Cloud Director アプライアンスのデプロイ、VMware OVF Tool を使用した VMware Cloud 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 VMware Cloud Director アプライアンスのデプロイを参照してください。

VMware Cloud 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、VMware Cloud 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。サーバ グループを水平方向に拡張するには、アプリケーション セルをさらにデプロイします。図 3-1. VMware Cloud Director アプライアンス データベース HA クラスタ図を参照してください。

図 3-1. VMware Cloud 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 VMware Cloud 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 VMware Cloud 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 VMware Cloud 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、VMware Cloud 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、VMware Cloud 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 VMware Cloud 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 VMware Cloud 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 VMware Cloud 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。

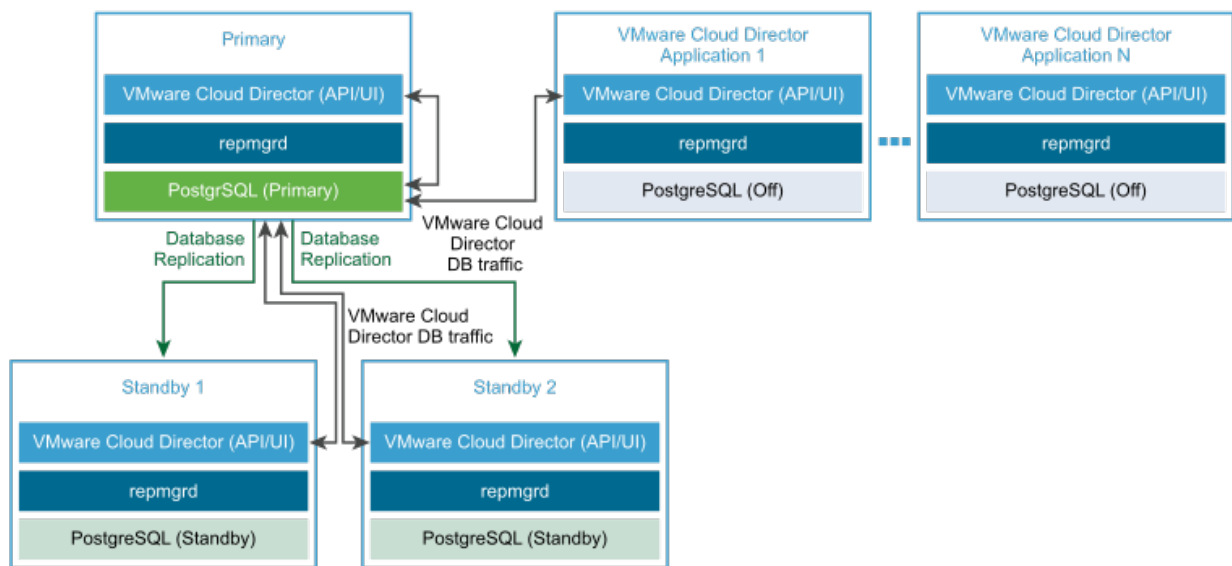
注： スタンバイ アプライアンスを最初にデプロイした後、Replication Manager はプライマリ アプライアンス データベースと自身のデータベースの同期を開始します。この期間中、VMware Cloud Director データベースは使用できないため、VMware Cloud Director のユーザー インターフェイスも使用できません。

- 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。

VMware Cloud Director アプライアンス クラスタの健全性とフェイルオーバー モードの表示を参照してください。

- 5 (オプション) VMware Cloud Director アプリケーション セルとして、VMware Cloud 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。VMware Cloud 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。



注： クラスタが自動フェイルオーバー用に構成されている場合は、追加セルをデプロイした後、アプライアンス API を使用して、そのフェイルオーバー モードを Automatic に設定する必要があります。[VMware Cloud Director アプライアンス API] を参照してください。新しいセルのデフォルトのフェイルオーバー モードは Manual です。クラスタのノード間でフェイルオーバー モードが不整合な状態の場合は、クラスタのフェイルオーバー モードは Indeterminate です。Indeterminate モードでは、元のプライマリ セルをフォローするノード間でクラスタの状態が不整合になる可能性があります。クラスタのフェイルオーバー モードを表示するには、VMware Cloud Director アプライアンス クラスタの健全性とフェイルオーバー モードの表示を参照してください。

データベース HA 構成を含まない VMware Cloud 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、VMware Cloud 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。

データベース HA 構成を含まない VMware Cloud 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 VMware Cloud 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、VMware Cloud 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、VMware Cloud 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。

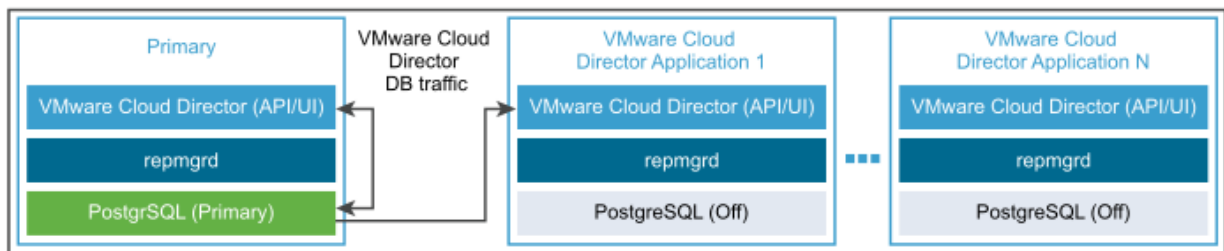
- a VMware Cloud Director サービスの健全性を確認するには、システム管理者の認証情報を使用して、`https://primary_eth0_ip_address/provider` にある VMware Cloud Director Service Provider Admin Portal にログインします。

- 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) VMware Cloud Director アプリケーション セルとして、VMware Cloud 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。VMware Cloud 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。



VMware Cloud Director アプライアンスの自動フェイルオーバー

VMware Cloud Director 10.1 以降では、プライマリ データベース サービスに障害が発生した場合、VMware Cloud Director を有効にして、新しいプライマリへの自動フェイルオーバーを実行できます。

自動フェイルオーバーによって、プライマリ データベース サービスが何らかの理由で機能できない場合に、管理者がフェイルオーバー アクションを開始する必要がなくなります。デフォルトでは、フェイルオーバー モードは手動に設定されています。フェイルオーバー モードは、VMware Cloud Director アプライアンス API を使用して、自動または手動に設定できます。『VMware Cloud Director アプライアンス API スキーマ リファレンス』を参照してください。

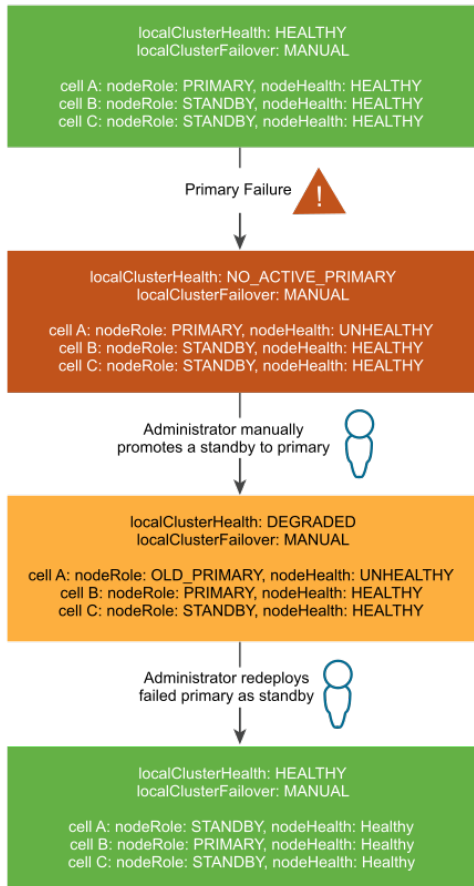
注： クラスタが自動フェイルオーバー用に構成されている場合は、追加セルをデプロイした後、アプライアンス API を使用して、そのフェイルオーバー モードを Automatic に設定する必要があります。[[VMware Cloud Director アプライアンス API](#)] を参照してください。新しいセルのデフォルトのフェイルオーバー モードは Manual です。クラスタのノード間でフェイルオーバー モードが不整合な状態の場合は、クラスタのフェイルオーバー モードは Indeterminate です。Indeterminate モードでは、元のプライマリ セルをフォローするノード間でクラスタの状態が不整合になる可能性があります。クラスタのフェイルオーバー モードを表示するには、[VMware Cloud Director アプライアンス クラスタの健全性とフェイルオーバー モードの表示](#)を参照してください。

環境内に 2 つ以上のアクティブなスタンバイ セルがある場合、プライマリ データベースに障害が発生すると、データベースのフェイルオーバーが自動的に開始されます。フェイルオーバー後に、新しいプライマリ データベースが更新できるようになるには、1 つ以上のアクティブなスタンバイが必要です。通常の場合では、VMware Cloud Director アプライアンスのデプロイには、常に 2 つ以上のアクティブなスタンバイが必要です。たとえば、プライマリの障害やいずれかのスタンバイの昇格などのため、短期間、アクティブなスタンバイが 1 つのみの場合は、障害が発生した古いプライマリを速やかに新しいスタンバイに置き換える必要があります。

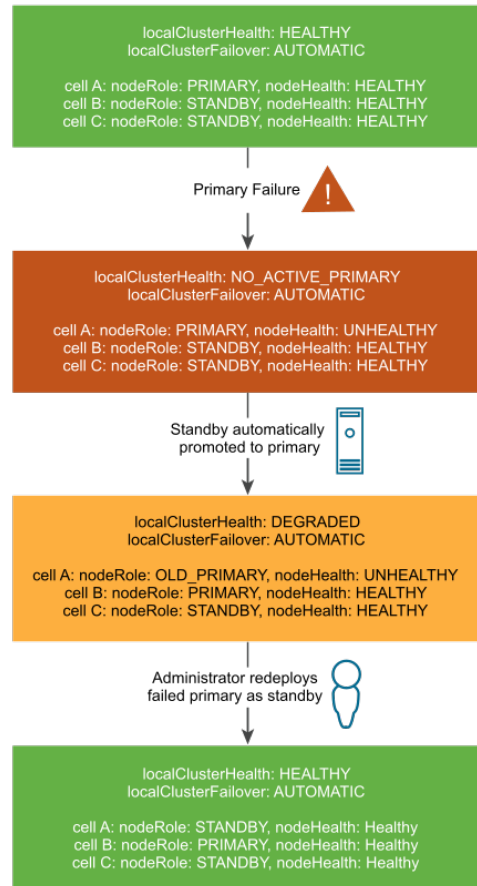
アクティブなプライマリと 2 つ以上のアクティブなスタンバイ セルがある場合、クラスタは Healthy 状態であると見なされます。アクティブなプライマリと 1 つのみのアクティブなスタンバイが存在する場合、クラスタは Degraded 状態です。クラスタが Degraded 状態のときに別のデータベース障害が発生した場合は、別のスタンバイがオンラインになるまで、プライマリを更新できません。プライマリ データベースが更新できない場合、VMware Cloud Director は使用できません。これは、プライマリ データベースからのストリーミング複製を処理するための 1 つ以上のアクティブなスタンバイが存在するようになるまで、VMware Cloud Director セルがデータベースを更新できないためです。Healthy と Degraded のクラスタの概念は、有効にするフェイルオーバーが手動の場合も自動の場合も同じです。

図 3-2. 手動および自動 VMware Cloud Director アプライアンス フェイルオーバー

Manual VMware Cloud Director Appliance Failover



Automatic VMware Cloud Director Appliance Failover



障害のあるプライマリ セルの自動フェンス

プライマリ セルに障害が発生した後に新しいプライマリ セルが昇格された場合、VMware Cloud Director は元のプライマリが再起動しないよう自動的にフェンスします。

フェイルオーバーの場合、障害のあるプライマリ データベースが新しいプライマリ セルの昇格後に再起動すると、VMware Cloud Director は元のプライマリを自動的にフェンスします。この自動処理により、2 つのアクティブなデータベースが相互に分断される可能性があるスプリットブレイン シンドロームを回避します。フェンスの自動処理により、元のプライマリ ノード上の vpostgres サービスは停止され、無効にされます。その後、障害のあるプライマリをスタンバイ セルとして再デプロイし、クラスタの健全性を Healthy にリストアできます。

クラスタの健全性ステータスおよびフェイルオーバー モードの表示の詳細については、[VMware Cloud Director アプライアンス クラスタの健全性とフェイルオーバー モードの表示](#)を参照してください。

VMware Cloud Director アプライアンスのデプロイの準備

VMware Cloud 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。

VMware Cloud Director アプライアンス用の転送サーバ ストレージの準備

NFS またはその他の共有ストレージ ボリュームは、VMware Cloud Director サーバ グループ内のすべてのサーバからアクセスできるようにする必要があります。VMware Cloud Director は、転送サーバ ストレージを、アプライアンス クラスタの管理に使用するほか、アップロード、ダウンロード、および外部で公開またはサブスクライブされたカタログ アイテムの一時ストレージとして使用します。

重要： VMware Cloud 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。VMware Cloud Director アプライアンスは、ディレクトリの権限と所有権など、デプロイ中に NFS 共有のほとんどの詳細も検証します。有効な NFS マウント ポイントが存在し、VMware Cloud Director アプライアンス インスタンスにアクセスできることを確認する必要があります。

サーバ グループの各メンバーは、このボリュームを同じマウントポイント (`/opt/vmware/vcloud-director/data/transfer`) にマウントします。このボリュームの領域は、次のような多くの方法で使用されます。

- 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 アイテムがこのボリュ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。
- VMware Cloud Director は、アプライアンス データベースのバックアップを転送共有の `pgdb-backup` ディレクトリに格納します。これらのバックアップ バンドルは、大きな容量を使用する場合があります。
- 複数セルのログ バンドル コレクタは、この容量を占有します。
- アプライアンス ノードのデータと `response.properties` ファイルはこの容量を占有します。

注： 転送サーバ ストレージのボリュームには、将来の拡張のための容量が必要です。

注： NFS のダウンタイムにより、VMware Cloud Director アプライアンス クラスタの機能が誤動作することがあります。NFS が停止している場合、またはアクセスできない場合、アプライアンス管理ユーザー インターフェイスは応答しません。影響を受ける可能性のあるその他の機能として、障害が発生したプライマリ セルのフェンス、スイッチオーバー、スタンバイ セルの昇格などがあります。

注： NFS に Ubuntu または Debian ベースの Linux ディストリビューションを使用すると、データベース バックアップの作成が失敗する可能性があります。

共有ストレージ オプション

従来の Linux ベースの NFS サーバやほかのソリューション（Microsoft Windows Server、VMware vSAN File Service の NFS 機能など）では、共有ストレージを使用できます。vSAN 7.0 以降では、vSAN File Service 機能で NFS 3.0 および NFS 4.1 プロトコルを使用して、NFS 共有をエクスポートすることができます。vSAN File Service の詳細については、[VMware vSphere 製品のドキュメント](#)の『Administering VMware vSAN』ガイドを参照してください。

NFS サーバを構成するための要件

NFS サーバの構成には、VMware Cloud 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、VMware Cloud 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、VMware Cloud 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。

Linux NFS サーバの例

Linux NFS サーバに、VMware Cloud 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、vCD-Cell2-IP、vCD-Cell3-IP という名前の 3 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メソッドは、no_root_squash メソッドです。/etc/exports ファイルに次の行を追加する必要があります。

```
/nfs/vCDspace vCD_Cell1_IP_Address(rw,sync,no_subtree_check,no_root_squash)
/nfs/vCDspace vCD_Cell2_IP_Address(rw,sync,no_subtree_check,no_root_squash)
/nfs/vCDspace vCD_Cell3_IP_Address(rw,sync,no_subtree_check,no_root_squash)
```

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。

VMware Cloud Director サーバ グループ内のサーバのすべてがこの NFS 共有をマウントできるように、NFS サーバの /etc/exports ファイルに、これらのサーバに対応するエントリが必要になります。NFS サーバ上の /etc/exports ファイルに変更を加えた後、exportfs -a を実行して、すべての NFS 共有を再度エクスポートします。

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

VMware Cloud 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 VMware Cloud 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。VMware Cloud 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 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、[VMware Cloud 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、VMware Cloud 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。VMware Cloud 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、[Linux での VMware Cloud 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、VMware Cloud Director インストールで VMware Cloud 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。

VMware Cloud 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 クラスター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。

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

VMware Cloud 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。

VMware Cloud 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、[VMware Cloud 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、VMware Cloud 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。VMware Cloud 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、[Linux での VMware Cloud 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

VMware Cloud 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、『VMware Cloud 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、『VMware Cloud 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、『VMware Cloud Director Service Provider Admin Portal Guide』を参照してください。

VMware Cloud Director アプライアンスのデプロイと初期構成

VMware Cloud 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、VMware Cloud Director サーバ グループを作成できます。vSphere Client または VMware OVF Tool を使用した VMware Cloud Director アプライアンスをデプロイします。

重要： Linux 上の VMware Cloud Director インストールおよび VMware Cloud 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。

VMware Cloud Director アプライアンスは、VMware Cloud 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 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-9.7.0.0-9229800_OVA10.ova

VMware Cloud 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
- VMware Cloud 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 VMware Cloud 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： VMware Cloud 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、VMware Cloud 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、VMware Cloud 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。VMware Cloud 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、VMware Cloud 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、VMware Cloud 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 VMware Cloud 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： VMware Cloud 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 VMware Cloud 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

VMware Cloud 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。

VMware Cloud 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。

バージョン 10.1 以降では、サービス プロバイダとテナントは VMware Cloud Director API を使用してリモート サーバへの接続をテストし、サーバ ID を SSL ハンドシェイクの一部として検証できます。VMware Cloud Director ネットワーク接続を保護するために、VMware Cloud Director API を使用して接続テストを行っているテナントからは到達できない内部ホストの拒否リストを構成します。VMware Cloud Director のインストールまたはアップグレードの後、テナントに VMware Cloud Director へのアクセスを許可する前に、拒否リストを構成します。[テスト接続拒否リストの構成](#)を参照してください。

VMware Cloud 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、VMware Cloud 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、VMware Cloud 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、VMware Cloud 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。

VMware Cloud 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、VMware Cloud 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。

VMware Cloud 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 VMware Cloud Director のデプロイ	いいえ	いいえ	はい
VMware Cloud 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

	中	大	特大 (VVD)
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： VMware Cloud 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 VMware Cloud 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
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

VMware Cloud 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、VMware Cloud Director セルでデータベースへの接続が切断される場合があります。

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 VMware Cloud 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-XXXXXX]
Timeout: Pool empty.Unable to fetch a connection in 20 seconds, none
available.
```

また、VMware Cloud Director セルでデータベースへの接続が切断される場合があります。

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

VMware Cloud 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、VMware Cloud 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
```

VMware Cloud 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、VMware Cloud 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
```

VMware Cloud Director アプライアンスのデプロイの前提条件

VMware Cloud 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。

- VMware Cloud 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。[Linux での VMware Cloud Director の転送サーバ 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](#)。

VMware Cloud Director アプライアンスのデプロイ方法

- [vSphere Client を使用した VMware Cloud Director アプライアンスのデプロイ](#)
- [VMware OVF Tool を使用した VMware Cloud 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 VMware Cloud Director アプライアンスのデプロイ](#)

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

vSphere Client (HTML5) を使用して、VMware Cloud 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。OVF テンプレートをデプロイしたら、アプライアンス管理ユーザー インターフェイスで構成を完了する必要があります。

VMware Cloud 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。VMware Cloud 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 VMware Cloud Director 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 VMware Cloud Director インストールおよび VMware Cloud 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-*nnnnnnn*_OVF10.ova という形式の名前で配布されます。ここで *vv.v.v.v* は、製品バージョン、*nnnnnnn* 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。

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 VMware Cloud Director アプライアンスのデプロイ](#)を参照してください。

注： VMware Cloud Director への VMware Cloud 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

[VMware Cloud 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 VMware Cloud 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 ウィザードを開いて、OVF テンプレートをデプロイします。

2 VMware Cloud Director プライマリ アプライアンスの構成

プライマリ アプライアンスの OVF テンプレートをデプロイしたら、プライマリ VMware Cloud 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 インターフェイスの構成フェーズに進む必要があります。

3 VMware Cloud Director のスタンバイ セルとアプリケーション セルの構成

スタンバイ セルまたはアプライアンス セルの OVF テンプレートをデプロイしたら、デプロイするインスタンスのアプライアンス管理ユーザー インターフェイスの構成フェーズに進む必要があります。

次のステップ

- VMware Cloud 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。[Linux での VMware Cloud Director 用パブリック アドレスのカスタマイズ](#)を参照してください。
- VMware Cloud 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、VMware Cloud 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 VMware Cloud 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。

VMware Cloud 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 ウィザードを開いて、OVF テンプレートをデプロイします。

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 VMware Cloud 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 VMware Cloud 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）	<p>12 GB の RAM と 2 つの vCPU を搭載したアプライアンスを、VMware Cloud 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。</p> <p>プライマリ セルの組み込みデータベースは、VMware Cloud 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。</p>
プライマリ（大）	<ul style="list-style-type: none"> VMware Cloud Director 10.2.1 以降のバージョンは 24 GB の RAM と 8 つの vCPU を搭載したアプライアンスを、VMware Cloud 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。 VMware Cloud Director 10.2 は 24 GB の RAM と 4 つの vCPU を搭載したアプライアンスを、VMware Cloud 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。 <p>プライマリ セルの組み込みデータベースは、VMware Cloud 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。</p>
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 VMware Cloud 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> <ul style="list-style-type: none"> VMware Cloud Director 10.2.1 以降のバージョンは 24 GB の RAM と 8 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 VMware Cloud 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。 VMware Cloud Director 10.2 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 VMware Cloud 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>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>
Cloud Director セル アプリケーション	<ul style="list-style-type: none"> VMware Cloud Director 10.2.1 以降のバージョンは 8 GB の RAM と 4 つの vCPU を搭載したアプライアンスを、VMware Cloud 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。 VMware Cloud Director 10.2 は 8 GB の RAM と 2 つの vCPU を搭載したアプライアンスを、VMware Cloud 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>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： VMware Cloud 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構成できます。

- 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。

ソース ネットワーク リストが逆順になっていることがあります。各ソース ネットワークに対して正しいターゲット ネットワークを選択していることを確認します。

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 アドレスの割り当てと [IPv4] プロトコルを選択します。
- 11 [次へ] をクリックします。

VMware Cloud Director の詳細を設定するウィザードの [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。

- 12 [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構成します。

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>重要： 初期の root パスワードがキースタ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>FIPS モードを使用する場合は、アプライアンスの root パスワードを 14 文字以上にする必要があります。</p> <p>注： 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 ルート ログインの有効化	デフォルトでは無効になっています。

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>] を参照してください。

- 13 (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 ルートを経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。

- 14 [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 (<i>mydomain.com</i> 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 (<i>subdomain.example.com</i> など)。 注： [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。
<code>eth0</code> ネットワークの IP アドレス	<code>eth0</code> インターフェイスの IP アドレス。
<code>eth0</code> ネットワーク ネットマスク	<code>eth0</code> 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。
<code>eth1</code> ネットワークの IP アドレス	<code>eth1</code> インターフェイスの IP アドレス。
<code>eth1</code> ネットワーク ネットマスク	<code>eth1</code> 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。

- 15 [設定内容の確認] 画面で、VMware Cloud 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。
- [VMware Cloud Director プライマリ アプライアンスの構成](#)または [VMware Cloud Director のスタンバイ セルとアプリケーション セルの構成](#)。

VMware Cloud Director プライマリ アプライアンスの構成

プライマリ アプライアンスの OVF テンプレートをデプロイしたら、プライマリ VMware Cloud 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 インターフェイスの構成フェーズに進む必要があります。

前提条件

- [VMware Cloud Director アプライアンスのデプロイの開始](#)。

- 新しく作成した仮想マシンパワーオンします。
- VMware Cloud Director アプライアンス用の転送サーバ ストレージの準備のトピックについて理解しておきます。

手順

- Web ブラウザを開き、`https://Primary-Appliance-eth1-IP-Address:5480` に移動します。
- プライマリ 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ます。
[プライマリ アプライアンス システムのセットアップ] 画面が表示されます。
- [アプライアンスの設定] セクションでアプライアンスの詳細を構成し、[次へ] をクリックします。

設定	説明
転送ファイルの場所への NFS マウント	NFS 共有転送サーバ ストレージの場所。VMware Cloud Director によって場所が検証され、NFS マウントが検証されている場合は緑色のチェック マークが表示されます。
[vcloud] ユーザーのデータベース パスワード	vcloud PostgreSQL データベース ユーザーのパスワード。
データベース パスワードの確認	vcloud PostgreSQL データベース ユーザーのパスワードを確認します。
カスタマー エクスペリエンス向上プログラム への参加	VMware カスタマー エクスペリエンス向上プログラムへの参加を有効または無効にします。

- [管理者アカウント] セクションで、システム管理者の詳細を構成し、[次へ] をクリックします。

設定	説明
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。
パスワード	システム管理者アカウントのパスワード。パスワードは、6~128 文字の範囲内である必要があります。
パスワードを確認	システム管理者 アカウントのパスワードを確認します。
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。
メールアドレス	システム管理者のメール アドレス。

- [VMware Cloud Director 設定] セクションで、このインスタンスのインストールを構成します。

設定	説明
システム名	この VMware Cloud Director インストールに作成する vCenter Server フォルダの名前。
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 VMware Cloud 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 VMware Cloud 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 VMware Cloud 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。

- [送信] をクリックし、システムの設定が完了したら [OK] をクリックします。

結果

デプロイが成功すると、[組み込みデータベースの可用性] タブと [サービス] タブが表示されます。

次のステップ

- [VMware Cloud Director アプライアンスのタイムゾーンの変更](#)
- スタンバイ セルまたはアプリケーション セルをデプロイします。 [VMware Cloud Director アプライアンスのデプロイの開始](#)を参照してください。
- [VMware Cloud Director のスタンバイ セルとアプリケーション セルの構成](#)

VMware Cloud Director のスタンバイ セルとアプリケーション セルの構成

スタンバイ セルまたはアプライアンス セルの OVF テンプレートをデプロイしたら、デプロイするインスタンスのアプライアンス管理ユーザー インターフェイスの構成フェーズに進む必要があります。

前提条件

- 1 スタンバイ セルまたはアプリケーション セルをデプロイします。 [VMware Cloud Director アプライアンスのデプロイの開始](#)を参照してください。
- 2 [VMware Cloud Director アプライアンス用の転送サーバ ストレージの準備](#)を参照してください。
- 3 新しく作成した仮想マシンパワーオンします。

手順

- 1 Web ブラウザを開き、`https://Cell-eth1-IP-Address:5480` に移動します。
- 2 スタンバイ セルまたはアプライアンス 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。
[システム セットアップ] 画面が表示されます。
- 3 転送ファイルの場所の NFS マウントを入力します。
- 4 [送信] をクリックし、システムの設定が完了したら [OK] をクリックします。

次のステップ

[VMware Cloud 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 VMware Cloud Director アプライアンスのデプロイ

VMware OVF Tool を使用して、VMware Cloud 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。

VMware Cloud 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。VMware Cloud 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 VMware Cloud Director 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 VMware Cloud Director インストールおよび VMware Cloud 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-*nnnnnnn*_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、*nnnnnnn* 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 VMware Cloud Director アプライアンスのデプロイ](#) を参照してください。

デプロイ コマンドを実行する前に、[VMware Cloud 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。

VMware Cloud Director 10.2 以降で VMware Cloud Director アプライアンスをデプロイするには、--X:enableHiddenProperties パラメータを含める必要があります。

注： プライマリ アプライアンスのデプロイ中に必要に応じて OVF 構成オプションを指定するか、またはデプロイ後にアプライアンス管理ユーザー インターフェイスを実行して構成を完了するかを選択できます。

VMware Cloud 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。
--X:enableHiddenProperties	該当なし	アプライアンスを構成するためのプロパティをすべて表示します。
--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。
--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"	portgroup_on_vc_for_eth0	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。 重要： 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。

オプション	値	説明
--net:"eth1 Network"	portgroup_on_vc_for_eth1	<p>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。</p> <p>重要: 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。</p>
--name	vm_name_on_vc	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"	eth0_ip_address	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"	eth1_ip_address	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"	dns_ip_address	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"	domain_name	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"	gateway_ip_address	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"	netmask	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"	netmask	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"	director_domain_names	<p>アプライアンスのドメイン検索パス。</p> <p>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。</p>
--prop:"vcloudconf.ceip_enabled.VMware_vCloud_Director"	true または false	<p>VMware カスタマー エクスペリエンス向上プログラムへの参加を有効または無効にします。デフォルトは true です。</p> <p>デプロイ後にアプライアンス管理ユーザー インターフェイスを実行してプライマリ アプライアンスの構成を完了する場合は、オプションです。</p>
--prop:"vcloudapp.enable_ssh.VMware_vCloud_Director"	true または false	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"	true または false	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"	host_ip_address:nfs_mount_path	<p>外部 NFS サーバの IP アドレスとエクスポートパス。</p> <p>プライマリ セルにのみ使用されます。</p>
--prop:"vcloudapp.ntp-server.VMware_vCloud_Director"	ntp_server_address	タイム サーバの IP アドレス。

オプション	値	説明
<code>--prop:"vcloudapp.varoot-password.VMware_vCloudDirector"</code>	<code>VMware_vCloudDirector</code>	<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>重要： 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>
<code>--prop:"vcloudconf.db_pwd.VMware_vCloudDirector"</code>	<code>VMware_vCloudDirector</code>	<p>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。</p> <p>デプロイ後にアプライアンス管理ユーザー インターフェイスを実行してプライマリ アプライアンスの構成を完了する場合は、オプションです。</p>
<code>--prop:"vcloudconf.admin_email.VMware_vCloudDirector"</code>	<code>VMware_vCloudDirector</code>	<p>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。</p> <p>デプロイ後にアプライアンス管理ユーザー インターフェイスを実行してプライマリ アプライアンスの構成を完了する場合は、オプションです。</p>
<code>--prop:"vcloudconf.admin_fname.VMware_vCloudDirector"</code>	<code>VMware_vCloudDirector</code>	<p>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。</p> <p>デプロイ後にアプライアンス管理ユーザー インターフェイスを実行してプライマリ アプライアンスの構成を完了する場合は、オプションです。</p>
<code>--prop:"vcloudconf.admin_pwd.VMware_vCloudDirector"</code>	<code>VMware_vCloudDirector</code>	<p>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。</p> <p>デプロイ後にアプライアンス管理ユーザー インターフェイスを実行してプライマリ アプライアンスの構成を完了する場合は、オプションです。</p>
<code>--prop:"vcloudconf.admin_uname.VMware_vCloudDirector"</code>	<code>VMware_vCloudDirector</code>	<p>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。</p> <p>デプロイ後にアプライアンス管理ユーザー インターフェイスを実行してプライマリ アプライアンスの構成を完了する場合は、オプションです。</p>
<code>--prop:"vcloudconf.inst_id.VMware_vCloudDirector"</code>	<code>VMware_vCloudDirector</code>	<p>VMware Cloud Director インストール ID。プライマリ セルにのみ使用されます。</p> <p>デプロイ後にアプライアンス管理ユーザー インターフェイスを実行してプライマリ アプライアンスの構成を完了する場合は、オプションです。</p>
<code>--prop:"vcloudconf.sys_name.VMware_vCloudDirector"</code>	<code>VMware_vCloudDirector</code>	<p>この VMware Cloud Director インストールに作成する vCenter Server フォルダの名前。デプロイ後にアプライアンス管理ユーザー インターフェイスを実行してプライマリ アプライアンスの構成を完了する場合は、オプションです。</p>

オプション	値	説明
<code>--prop:"vcloudnet.routes0.VMware_vCloudDirector" cidr,</code> <code>ip_address1,</code> <code>ip_address2, ...</code>		オプション。eth0 インターフェイスのスタティック 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、 172.16.100.253 172.16.100/19, 172.16.200.253 のようになります。
<code>--prop:"vcloudnet.routes1.VMware_vCloudDirector" cidr,</code> <code>ip_address1,</code> <code>ip_address2, ...</code>		オプション。eth1 インターフェイスのスタティック 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、 172.16.100.253 172.16.100/19, 172.16.200.253 のようになります。

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。ラボ システムまたはテスト システムに適している VMware Cloud 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。</p> <ul style="list-style-type: none"> ■ 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、VMware Cloud 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、VMware Cloud 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。 ■ primary-large : <ul style="list-style-type: none"> ■ VMware Cloud Director 10.2.1 以降のバージョンは 24 GB の RAM と 8 つの vCPU を搭載したアプライアンスを、VMware Cloud 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。 ■ VMware Cloud Director 10.2 は 24 GB の RAM と 4 つの vCPU を搭載したアプライアンスを、VMware Cloud 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、VMware Cloud 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。 ■ 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 VMware Cloud 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。 ■ standby-large : <ul style="list-style-type: none"> ■ VMware Cloud Director 10.2.1 以降のバージョンは 24 GB の RAM と 8 つの vCPU を搭載したアプライア

オプション	値	説明
		<p>ンスを、データベース高可用性構成の VMware Cloud 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> <ul style="list-style-type: none"> ■ VMware Cloud Director 10.2 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 VMware Cloud 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>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> <ul style="list-style-type: none"> ■ cell : ■ VMware Cloud Director 10.2.1 以降のバージョンは 8 GB の RAM と 4 つの vCPU を搭載したアプライアンスを、VMware Cloud 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。 ■ VMware Cloud Director 10.2 は 8 GB の RAM と 2 つの vCPU を搭載したアプライアンスを、VMware Cloud 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>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> <p>重要： VMware Cloud 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。</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	path_to_ova	デプロイ後、仮想マシンをパワーオンします。

本番環境用プライマリ VMware Cloud 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 \
--X:enableHiddenProperties \
--datastore='datastore6' \
--allowAllExtraConfig \
--net:"eth0 Network"="My_UI_API_Network" \
--net:"eth1 Network"="My_Internal_DB_Services_Network" \
--name=MyAppliance \
--diskMode=thick \
--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-large" \
--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
```

本番環境用スタンバイ VMware Cloud 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 \
--X:enableHiddenProperties \
--datastore='datastore6' \
```

```
--allowAllExtraConfig \
--net:"eth0 Network"="My_UI_API_Network" \
--net:"eth1 Network"="My_Internal_DB_Services_Network" \
--name=MySecondAppliance \
--diskMode=thick \
--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-large" \
--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
```

VMware Cloud Director アプライアンスのデプロイ後の作業

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。 [VMware Cloud 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。

アプライアンス管理ユーザー インターフェイスを使用して、プライマリ アプライアンスを構成します。 [VMware Cloud Director プライマリ アプライアンスの構成](#)を参照してください。

アプライアンス管理ユーザー インターフェイスを使用して、スタンバイ セルとアプリケーション セルを構成します。 [VMware Cloud Director のスタンバイ セルとアプリケーション セルの構成](#)を参照してください。

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 VMware Cloud 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、VMware Cloud 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、VMware Cloud Director アプライアンスをデプロイすると、VMware Cloud 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 VMware Cloud Director セルを構成します。

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 VMware Cloud 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構成できます。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、[VMware Cloud 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 VMware Cloud 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 VMware Cloud 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 VMware Cloud 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、[VMware Cloud 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 VMware Cloud Director アプライアンスへのインポート](#)を参照してください。
- 署名付きワイルドカード SSL 証明書を含むキーストアのキーストアタイプが JCEKS の場合、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、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 **vcloud** に変更します。

```
chown vcloud.vcloud /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 VMware Cloud 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。

- 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
```

- 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す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。

VMware Cloud 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 VMware Cloud 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 VMware Cloud 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。

VMware Cloud 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 VMware Cloud 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、VMware Cloud 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_password*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 VMware Cloud Director アプライアンスにインポートします。VMware Cloud Director は、keytool のコピーを /opt/vmware/vcloud-director/jre/bin/keytool に配置します。

手順

- 1 VMware Cloud 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。
- 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。

VMware Cloud Director アプライアンスをデプロイすると、VMware Cloud 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_password
```

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、発行者のコメントネーム (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： VMware Cloud 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： VMware Cloud 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 PKCS12 -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 PKCS12 -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 VMware Cloud 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 PKCS12 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 PKCS12 -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 PKCS12 -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 PKCS12 -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 PKCS12 -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 PKCS12 -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 VMware Cloud 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、VMware Cloud Director アプライアンスで 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
```

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 VMware Cloud 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 VMware Cloud 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 VMware Cloud 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 VMware Cloud 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 VMware Cloud 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 VMware Cloud 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 VMware Cloud Director アプライアンスにインポートします。VMware Cloud 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 VMware Cloud 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。
- 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.p12 -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.p12 -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 certificates.ks 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 PKCS12 -srckeystore http.p12
-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 PKCS12 -srckeystore consoleproxy.p12
-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 PKCS12 -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 VMware Cloud 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、VMware Cloud 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 VMware Cloud 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 VMware Cloud 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 VMware Cloud 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 VMware Cloud 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。

VMware Cloud Director アプライアンスのデプロイ後の作業

VMware Cloud 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 を構成し、データベース上の一部のパラメータを調整できます。

VMware Cloud 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。

注： クラスタが自動フェイルオーバー用に構成されている場合は、追加セルをデプロイした後、アプライアンス API を使用して、そのフェイルオーバー モードを Automatic に設定する必要があります。[VMware Cloud Director アプライアンス API] を参照してください。新しいセルのデフォルトのフェイルオーバー モードは Manual です。クラスタのノード間でフェイルオーバー モードが不整合な状態の場合は、クラスタのフェイルオーバー モードは Indeterminate です。Indeterminate モードでは、元のプライマリ セルをフォローするノード間でクラスタの状態が不整合になる可能性があります。クラスタのフェイルオーバー モードを表示するには、[VMware Cloud Director アプライアンス クラスタの健全性とフェイルオーバー モードの表示](#)を参照してください。

バージョン 10.1 以降では、サービス プロバイダとテナントは VMware Cloud Director API を使用してリモート サーバへの接続をテストし、サーバ ID を SSL ハンドシェイクの一部として検証できます。VMware Cloud Director ネットワーク接続を保護するために、VMware Cloud Director API を使用して接続テストを行っているテナントからは到達できない内部ホストの拒否リストを構成します。VMware Cloud Director のインストールまたはアップグレードの後、テナントに VMware Cloud Director へのアクセスを許可する前に、拒否リストを構成します。[テスト接続拒否リストの構成](#)を参照してください。

VMware Cloud Director アプライアンスのタイムゾーンの変更

VMware Cloud 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 VMware Cloud 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

- VMware Cloud Director アプライアンスをデプロイします。 [VMware Cloud Director アプライアンスのデプロイと初期構成](#)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 VMware Cloud 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 VMware Cloud 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 VMware Cloud 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 VMware Cloud 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。

VMware Cloud Director アプライアンスの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、VMware Cloud Director Web ポータル、VMware Cloud Director 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。

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、VMware Cloud 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。6 を参照してください。

前提条件

システム管理者としてログインしていることを確認します。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 Service Provider Admin Portal の上部ナビゲーション バーで [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 公開エンドポイントをカスタマイズするには、[編集] をクリックします。
- 4 VMware Cloud 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 HTTPS（セキュア）接続用のカスタムの VMware Cloud 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す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 VMware Cloud 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) Cloud Director 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 VMware Cloud Director API に、`http://vcloud.example.com/cloudapi` から VMware Cloud Director 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 VMware Cloud Director API に、`https://vcloud.example.com/cloudapi` から VMware Cloud Director 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 VMware Cloud 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 VMware Cloud 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、コンソール プロキシ サービスにカスタム ポート 8443 を使用して、FQDN または IP アドレスで指定された VMware Cloud Director アプライアンス `eth0` NIC の完全修飾ドメイン名 (FQDN) です。

たとえば、VMware Cloud 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。

VMware Cloud 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

VMware Cloud 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。VMware Cloud 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 VMware Cloud 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、VMware Cloud 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、『VMware Cloud 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、VMware Cloud 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@cell11 /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、「[5 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) VMware Cloud 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@cell11 /opt/vmware/vcloud-director/
bin]# ./cell-management-tool cassandra --add-rollup \ --username admin --password
'P@55w0rd'
```

- 3 各 VMware Cloud Director セルを再起動します。

RabbitMQ AMQP ブローカのインストールおよび構成

ブロック タスク、通知、VMware Cloud Director API 拡張機能 (Container Service Extension (CSE) や VMware Cloud Director App Launchpad など) を使用するには、RabbitMQ AMQP ブローカをインストールし構成する必要があります。

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。VMware Cloud 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。

VMware Cloud Director では、通知を構成する際に、RabbitMQ AMQP ブローカの代わりに MQTT クライアントを使用できます。 [MQTT クライアントを使用したイベント、タスク、およびメトリックへのサブスクライブ](#)を参照してください。

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、『VMware Cloud 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 VMware Cloud 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 VMware Cloud 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。非 SSL では、デフォルトは 5672 です。SSL/TLS のデフォルト ポートは 5671 です。
 - 通信プロトコルは TCP 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、VMware Cloud 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。VMware Cloud 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。

VMware Cloud Director AMQP サービスで SSL を有効にするには、『VMware Cloud Director Service Provider Admin Portal Guide』の [AMQP ブローカの構成](#) の情報を参照してください。

VMware Cloud Director アプライアンスの root パスワードの変更

VMware Cloud Director アプライアンスの root パスワードを変更する場合は、新しいパスワードを使用するようにアプライアンス証明書キーストアも更新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。VMware Cloud Director は keytool のコピーを /opt/vmware/vcloud-director/jre/bin/keytool に配置します。
- ワイルドカード証明書を使用していて、これらの証明書を NFS 共有転送ストレージに格納している場合に、これらの証明書が確実に更新されるようにするには、[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 VMware Cloud Director アプライアンスのデプロイ](#) に記載されている手順を実行します。

手順

- 1 VMware Cloud 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。
- 2 passwd コマンドを実行し、root ユーザーのパスワードを変更します。

```
passwd root
```

注： FIPS モードが有効になっている場合、アプライアンスの root パスワードは 14 文字以上にする必要があります。

注： root パスワードがすでに期限切れの場合は、root として VMware Cloud Director アプライアンス コンソールに初めてログインした際に、VMware Cloud Director から root パスワードの設定を要求されます。

- 3 コマンドを実行して、既存の証明書キーストア ファイルをバックアップします。

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

- 4 新しい証明書キーストアを生成するには、`keytool` コマンドを実行します。

```
keytool -importkeystore -srckeystore /opt/vmware/vcloud-director/certificates.ks
-srcstoretype PKCS12 -srcstorepass old_root_password -destkeystore /opt/vmware/vcloud-
director/certificates-new.ks -deststoretype PKCS12 -deststorepass new_root_password
-destkeypass new_root_password
```

注： VMware Cloud Director 10.2 以降では、VMware Cloud Director アプライアンスのデフォルトの証明書キーストア タイプは PKCS12 です。バージョン 10.2 にアップグレードされたアプライアンスのバージョンを使用している場合は、JCEKS を `-srcstoretype` および `-deststoretype` として使用します。

```
keytool -importkeystore -srckeystore /opt/vmware/vcloud-director/certificates.ks
-srcstoretype JCEKS -srcstorepass old_root_password -destkeystore /opt/vmware/vcloud-
director/certificates-new.ks -deststoretype JCEKS -deststorepass new_root_password
-destkeypass new_root_password
```

- 5 コマンドを実行して、古い証明書キーストア ファイルを新しいファイルに置き換えます。

```
mv /opt/vmware/vcloud-director/certificates-new.ks /opt/vmware/vcloud-director/
certificates.ks
```

- 6 キーストア ファイルのユーザーおよびグループ所有権を確認するには、`chown` コマンドを実行します。

```
chown vcloud.vcloud /opt/vmware/vcloud-director/certificates.ks
```

- 7 キーストアの新しいパスワードを使用するには、VMware Cloud Director サーバ構成を更新します。

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

次のステップ

クラスタ内の各アプライアンスにこの手順を繰り返します。

重要： すべてのアプライアンスで同じ root パスワードが共有されている必要があります。新しくデプロイされたアプライアンスでは、新しい root パスワードを使用する必要があります。

VMware Cloud Director アプライアンスのアップグレードと移行

バージョン 9.7 以降、VMware Cloud 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。VMware Cloud Director アプライアンスを新しいバージョンにアップグレードできます。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 VMware Cloud Director を、バージョン 10.0 以降の VMware Cloud Director アプライアンス環境で構成されている VMware Cloud Director 環境に移行できます。

VMware Cloud Director アプライアンスのアップグレード

VMware Cloud Director アプライアンスのバージョン 9.7 からバージョン 10.2 へのアップグレードについては、[アップデート パッケージを使用した VMware Cloud 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。

VMware Cloud 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。

VMware Cloud 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。

- VMware Cloud 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。
- VMware Cloud Director と直接通信するサードパーティ製コンポーネント。

VMware Cloud 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。VMware Cloud 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、VMware Cloud 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。[VMware Cloud Director のアップグレード後](#)を参照してください。

1 台以上の VMware Cloud Director サーバをアップグレードしてから、VMware Cloud 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 VMware Cloud 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、VMware Cloud 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せん。

- 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 VMware Cloud 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。

バージョン 10.1 以降では、サービス プロバイダとテナントは VMware Cloud Director API を使用してリモート サーバへの接続をテストし、サーバ ID を SSL ハンドシェイクの一部として検証できます。VMware Cloud Director ネットワーク接続を保護するために、VMware Cloud Director API を使用して接続テストを行っているテナントからは到達できない内部ホストの拒否リストを構成します。VMware Cloud Director のインストールまたはアップグレードの後、テナントに VMware Cloud Director へのアクセスを許可する前に、拒否リストを構成します。[テスト接続拒否リストの構成](#)を参照してください。

重要： バージョン 10.1 以降にアップグレードすると、VMware Cloud Director は常に、自身に接続されているすべてのインフラストラクチャ エンドポイントの証明書を検証します。これは、VMware Cloud Director での SSL 証明書の管理方法が変更されたためです。アップグレード前に証明書を VMware Cloud Director にインポートしていない場合は、vCenter Server と NSX の接続が、SSL 検証の問題が原因の接続エラーで失敗したと表示されることがあります。この場合、アップグレード後に、次の 2 つの方法のいずれかを実行できます。

- 1 セル管理ツールで `trust-infra-certs` コマンドを実行して、すべての証明書を中央の証明書ストアに自動的にインポートします。[vSphere リソースからのエンドポイント証明書のインポート](#)を参照してください。
- 2 Service Provider Admin Portal ユーザー インターフェイスで、各 vCenter Server および NSX インスタンスを選択し、証明書を承認する際に資格情報を再入力します。

VMware Cloud Director アプライアンスの移行

既存の VMware Cloud Director サーバ グループが VMware Cloud 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 VMware Cloud 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 VMware Cloud 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。

VMware Cloud 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、VMware Cloud Director 10.2 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、[Linux での VMware Cloud Director のアップグレード](#)を参照してください。

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
	組み込みの PostgreSQL データベースを使用する VMware Cloud Director アプライアンス 10.2
外部 Microsoft SQL Server データベースを使用する Linux 上の VMware Cloud Director 9.7	<ol style="list-style-type: none"> 1 VMware Cloud Director アプライアンス 9.7 に移行します。 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を参照してください。 2 環境を VMware Cloud Director アプライアンス 10.2 にアップグレードします。アップデート パッケージを使用した VMware Cloud 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。
外部 PostgreSQL データベースを使用する Linux 上の VMware Cloud Director 9.7	<ol style="list-style-type: none"> 1 VMware Cloud Director アプライアンス 9.7 に移行します。 Migrating vCloud Director with an External PostgreSQL Database to vCloud Director Applianceを参照してください。 2 環境を VMware Cloud Director アプライアンス 10.2 にアップグレードします。アップデート パッケージを使用した VMware Cloud 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。
外部 PostgreSQL データベースを使用する Linux 上の VMware Cloud Director 10.0	<ol style="list-style-type: none"> 1 VMware Cloud Director アプライアンス 10.0 に移行します。 Migrating vCloud Director with an External PostgreSQL Database to vCloud Director Applianceを参照してください。 2 環境を VMware Cloud Director アプライアンス 10.2 にアップグレードします。アップデート パッケージを使用した VMware Cloud 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。
外部 PostgreSQL データベースを使用する Linux 上の VMware Cloud Director 10.1	<ol style="list-style-type: none"> 1 VMware Cloud Director アプライアンス 10.1 に移行します。 外部 PostgreSQL データベースを使用する VMware Cloud Director の VMware Cloud Director アプライアンスへの移行を参照してください。 2 環境を VMware Cloud Director アプライアンス 10.2 にアップグレードします。アップデート パッケージを使用した VMware Cloud 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。
組み込みの PostgreSQL データベースを使用する VMware Cloud Director アプライアンス 9.7、10.0、および 10.1	環境を VMware Cloud Director アプライアンス 10.2 にアップグレードします。 アップデート パッケージを使用した VMware Cloud 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。

アップデート パッケージを使用した VMware Cloud Director アプライアンスのアップグレード

アップデート パッケージを使用することにより、VMware Cloud Director アプライアンスの最新バージョンへのアップグレードや、VMware Cloud Director アプライアンスへのパッチ適用ができます。

VMware Cloud Director アプライアンス環境へのアップグレード中に VMware Cloud 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 VMware Cloud Director アプライアンスをアップグレードし、VMware Cloud 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 VMware Cloud Director アプライアンスで VMware Cloud Director サービスを停止するまで、VMware Cloud Director サーバ グループ内の動作中のセルの数は減少します。VMware Cloud 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 VMware Cloud 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 VMware Cloud 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 VMware Cloud Director アプライアンスのスナップショットを作成します。

- 1 バージョン 10.1 以降からアップグレードするとき、またはパッチを適用するとき、プライマリ データベース サービスの障害発生時の自動フェイルオーバーが有効になっている場合は、アップグレードの間、フェイルオーバー モードを **Manual** に変更します。アップグレードが終わったら、フェイルオーバー モードを **Automatic** に設定できます。[VMware Cloud Director アプライアンスの自動フェイルオーバー](#)を参照してください。
- 2 データベース高可用性クラスタのプライマリ VMware Cloud 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。
- 3 プライマリ VMware Cloud 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。
- 4 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。
- 5 VMware Cloud 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。
- 6 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。[VMware Cloud Director アプライアンス クラスタの健全性とフェイルオーバー モードの表示](#)を参照してください。

手順

- 1 Web ブラウザで、VMware Cloud 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。

VMware Cloud Director は `VMware_Cloud_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_Cloud_Director_10.1.0.4424-14420378_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 -zxvf VMware_Cloud_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、VMware Cloud 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、VMware Cloud 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 VMware Cloud 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 VMware Cloud 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、VMware Cloud 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、VMware Cloud 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 VMware Cloud Director アプライアンスのロールバック](#)を参照してください。

VMware Update Repository を使用した VMware Cloud 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、VMware Cloud 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 以降にアップグレードするか、パッチを適用することができます。

注： VMware Update Repository は、VMware Cloud Director を最新バージョンの VMware Cloud 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。VMware Cloud Director を別のバージョンにアップグレードする場合は、[アップデート パッケージを使用した VMware Cloud 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。

VMware Cloud Director アプライアンス環境へのアップグレード中に VMware Cloud 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 VMware Cloud Director アプライアンスをアップグレードし、VMware Cloud 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 VMware Cloud Director アプライアンスで VMware Cloud Director サービスを停止するまで、VMware Cloud Director サーバ グループ内の動作中のセルの数は減少します。VMware Cloud 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 VMware Cloud 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 VMware Cloud 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 VMware Cloud Director アプライアンスのスナップショットを作成します。
 - バージョン 10.1 以降からアップグレードするとき、またはパッチを適用するときに、プライマリ データベース サービスの障害発生時の自動フェイルオーバーが有効になっている場合、アップグレードの間はフェイルオーバーモードを Manual に変更します。アップグレードが終わったら、フェイルオーバー モードを Automatic に設定できます。[VMware Cloud Director アプライアンスの自動フェイルオーバー](#)を参照してください。
 - データベース高可用性クラスタのプライマリ VMware Cloud 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。
 - プライマリ VMware Cloud 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。
 - 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。
 - VMware Cloud 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。
 - 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。[VMware Cloud Director アプライアンス クラスタの健全性とフェイルオーバー モードの表示](#)を参照してください。

- VMware Cloud 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、VMware Cloud 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。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 プライマリ 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。

- 3 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 ""
```

- 4 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。

- 5 次のコマンドを実行して、VMware Cloud 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
```

- 6 プライマリ アプライアンスから接続する場合は、VMware Cloud Director アプライアンス埋め込みデータベースをバックアップしてください。

```
/opt/vmware/appliance/bin/create-db-backup
```

注: アプライアンスは 1 回のみバックアップする必要があります。使用可能なアップグレードを適用した後は、アプライアンスをバックアップしないでください。

- 7 使用可能なアップグレードを適用します。

```
vamicli update --install latest
```

- 8 残りのスタンバイ セルとアプリケーション セルにログインし、各アプライアンスで手順 3、4、5、および 7 を繰り返します。

- 9 任意のアプライアンスから VMware Cloud 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
```

10 各 VMware Cloud 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、VMware Cloud 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、VMware Cloud 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 VMware Cloud Director アプライアンスのロールバック](#)を参照してください。
- `vamicli update --install latest` コマンドが失敗した場合は、[VMware Cloud Director の最新アップデートのインストールに失敗する](#)を参照してください。

アップグレードが失敗した場合の VMware Cloud Director アプライアンスのロールバック

VMware Cloud 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、VMware Cloud 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、VMware Cloud Director アプライアンス API を使用して、クラスタ内のスタンバイ ノードのノード ID をメモします。<http://code.vmware.com> の「VMware Cloud Director アプライアンス API スキーマ リファレンス」を参照してください。

- 1 プライマリ VMware Cloud 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 VMware Cloud Director アプライアンス セルをパワーオンします。
- 3 各 VMware Cloud 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 VMware Cloud Director サービスを停止します。

```
service vmware-vcd stop
```

- 5 プライマリ VMware Cloud 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 VMware Cloud 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 VMware Cloud Director アプライアンスのデプロイを参照してください。
- 9 各 VMware Cloud 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 VMware Cloud Director サービスを開始します。

```
service vmware-vcd start
```

外部 PostgreSQL データベースを使用した VMware Cloud Director の VMware Cloud Director アプライアンスへの移行

現在の VMware Cloud Director 環境で外部 PostgreSQL データベースを使用している場合は、VMware Cloud Director アプライアンス環境で構成される新しい VMware Cloud Director 環境に移行できます。現在の VMware Cloud Director 環境は、Linux 上の VMware Cloud Director インストール環境または VMware

Cloud 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 VMware Cloud 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 VMware Cloud Director 環境をアップグレードする
- VMware Cloud 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 VMware Cloud 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 VMware Cloud Director 環境をバージョン 10.2 にアップグレードします。

[Linux での VMware Cloud Director のアップグレード](#)を参照してください。

- 3 移行元の VMware Cloud 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 VMware Cloud Director 環境の各セルで以下のコマンドを実行して、VMware Cloud 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 VMware Cloud 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 VMware Cloud 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 VMware Cloud 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。

VMware Cloud Director アプライアンスのデプロイと初期構成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、VMware Cloud 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 VMware Cloud 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 でメモし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 VMware Cloud 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、VMware Cloud 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 7 a 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、VMware Cloud 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、[VMware Cloud Director アプライアンスに移行またはリストアすると VMware Cloud 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、VMware Cloud 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 VMware Cloud 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、VMware Cloud 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` 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 移行ソースからの既存の 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 VMware Cloud 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 VMware Cloud Director 環境に属する切断されたセルを削除します。
 - a 上部ナビゲーション バーの [リソース] で [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。

VMware Cloud 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 VMware Cloud 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 VMware Cloud 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。

VMware Cloud Director のアップグレード後

すべての VMware Cloud Director サーバと共有データベースをアップグレードした後、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、VMware Cloud 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： VMware Cloud Director では、詳細 Edge Gateway のみがサポートされます。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。

バージョン 10.1 以降では、サービス プロバイダとテナントは VMware Cloud Director API を使用してリモートサーバへの接続をテストし、サーバ ID を SSL ハンドシェイクの一部として検証できます。VMware Cloud Director ネットワーク接続を保護するために、VMware Cloud Director API を使用して接続テストを行っているテナントからは到達できない内部ホストの拒否リストを構成します。VMware Cloud Director のインストールまたはアップグレードの後、テナントに VMware Cloud Director へのアクセスを許可する前に、拒否リストを構成します。[テスト接続拒否リストの構成](#)を参照してください。

重要： バージョン 10.1 以降にアップグレードすると、VMware Cloud Director は常に、自身に接続されているすべてのインフラストラクチャ エンドポイントの証明書を検証します。これは、VMware Cloud Director での SSL 証明書の管理方法が変更されたためです。アップグレード前に証明書を VMware Cloud Director にインポートしていない場合は、vCenter Server と NSX の接続が、SSL 検証の問題が原因の接続エラーで失敗したと表示されることがあります。この場合、アップグレード後に、次の 2 つの方法のいずれかを実行できます。

- 1 セル管理ツールで `trust-infra-certs` コマンドを実行して、すべての証明書を中央の証明書ストアに自動的にインポートします。[vSphere リソースからのエンドポイント証明書のインポート](#)を参照してください。
- 2 Service Provider Admin Portal ユーザー インターフェイスで、各 vCenter Server および NSX インスタンスを選択し、証明書を承認する際に資格情報を再入力します。

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

VMware Cloud 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、VMware Cloud Director セルが実行中であるかどうかにかかわらず、VMware Cloud 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 VMware Cloud 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

VMware Cloud Director および NSX Manager のアップグレードが終わったら、VMware Cloud 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。
 - a VMware Cloud Director Service Provider Admin Portal の上部ナビゲーション バーで、[リソース] の下にある [vSphere リソース] を選択します。
 - b 左側のパネルで [vCenter Server インスタンス] をクリックします。
 - c 無効にする vCenter Server インスタンスの横にあるラジオ ボタンを選択して、[無効化] をクリックします。
 - d [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 VMware Cloud Director パブリック URL および証明書チェーンを確認します。
 - a 上部ナビゲーション バーで [管理] を選択します。
 - b 左側のパネルの [設定] で、[公開アドレス] をクリックします。
 - c 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 VMware Cloud Director で更新します。
 - a VMware Cloud Director Service Provider Admin Portal の上部ナビゲーション バーで、[リソース] の下にある [vSphere リソース] を選択します。
 - b 左側のパネルで [vCenter Server インスタンス] をクリックします。
 - c 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。
 - d [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 VMware Cloud 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/jp/>) を参照してください。
- VMware Cloud 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 VMware Cloud 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。
 - VMware Cloud Director または VMware Cloud Director 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、『VMware Cloud Director 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、VMware Cloud 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。

VMware Cloud Director アプライアンスの管理

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。

VMware Cloud 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。VMware Cloud 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。

注： クラスタが自動フェイルオーバー用に構成されている場合は、追加セルをデプロイした後、アプライアンス API を使用して、そのフェイルオーバー モードを Automatic に設定する必要があります。「[VMware Cloud Director アプライアンス API](#)」を参照してください。新しいセルのデフォルトのフェイルオーバー モードは Manual です。クラスタのノード間でフェイルオーバー モードが不整合な状態の場合は、クラスタのフェイルオーバー モードは Indeterminate です。Indeterminate モードでは、元のプライマリ セルをフォローするノード間でクラスタの状態が不整合になる可能性があります。クラスタのフェイルオーバー モードを表示するには、[VMware Cloud Director アプライアンス クラスタの健全性とフェイルオーバー モードの表示](#)を参照してください。

VMware Cloud 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

VMware Cloud 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 VMware Cloud Director 環境をリストアすることができます。

VMware Cloud 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 VMware Cloud 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 VMware Cloud 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 クライアントを使用して接続します。
- 2 次のコマンドを実行して、VMware Cloud 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
```

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.tar.gz` ファイルが表示されます。`.tar.gz` 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 VMware Cloud Director アプライアンス 10.2.1 以前の環境のリストア

高可用性データベース構成の VMware Cloud Director アプライアンス 10.2.1 以前の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。
[VMware Cloud 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。『[VMware Cloud Director アプライアンスのデプロイと初期構成](#)』を参照してください。
- 新しいアプライアンス クラスタで以前の環境の 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 VMware Cloud 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.tar.gz
```

/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、VMware Cloud Director バージョン 9.7.0.1 からバージョン 10.2.1 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、VMware Cloud 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、VMware Cloud Director バージョン 9.7.0.1 からバージョン 10.2.1 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、VMware Cloud Director バージョン 9.7.0.1 からバージョン 10.2.1 でのみ使用できます。

- 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、VMware Cloud 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 --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

/opt/vmware/vcloud-director/bin/cell-management-tool reconfigure-database --database-
ssl true
```

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。キーストアのパスワードは、アプライアンスのデプロイ中に使用した root パスワードである場合があります。
- --database-password オプションは、https://appliance_eth0_ip:5480 にある、VMware Cloud Director アプライアンス管理ユーザー インターフェイスでアプライアンスをセットアップするとき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、[VMware Cloud Director アプライアンスに移行またはリストアすると VMware Cloud 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、VMware Cloud 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。『[VMware Cloud Director アプライアンスのデプロイと初期構成](#)』を参照してください。
- 7 新しいアプライアンスで、置き換えている元のアプライアンスと異なる IP アドレスを使用する場合は、VMware Cloud Director サーバ グループの前面に配置されたロード バランサの構成を更新して、新しいアプライアンスの IP アドレスを含める必要があります。
- 8 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、VMware Cloud 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、VMware Cloud Director Service Provider Admin Portal を開きます。

- 手順 7 でロード バランサの構成を更新した場合は、サーバ グループのパブリック アドレスを使用して Service Provider Admin Portal にアクセスする必要があります。
- 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。
- 9 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 VMware Cloud Director 環境に属する切断されたセルを削除します。
- a 上部ナビゲーション バーの [リソース] で [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。
- 10 リストア前のフェイルオーバー モードが Automatic だった場合、それを再度 Automatic に設定するには、VMware Cloud Director アプライアンス API を使用する必要があります。

高可用性データベース構成の VMware Cloud Director アプライアンス 10.2.2 以降の環境のリストア

高可用性データベース構成の VMware Cloud Director アプライアンス 10.2.2 以降の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。
[VMware Cloud 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。『[VMware Cloud Director アプライアンスのデプロイと初期構成](#)』を参照してください。
- 新しいアプライアンス クラスタで以前の環境の 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 VMware Cloud 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.pem、 certificates.key、 proxycertificates.pem、 proxycertificates.key、 truststore.pem、 およびデータベース ファイル vcloud_date_time_format が表示されます。

注： truststore.pem ファイルは、VMware Cloud Director 10.2.2 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、VMware Cloud 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.pem、 certificates.key、 proxycertificates.pem、 proxycertificates.key、 および truststore.pem ファイルは /opt/vmware/vcloud-director/etc/ にあります。

注： truststore.pem ファイルは、VMware Cloud Director 10.2.2 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.pem ファイルは、VMware Cloud Director 10.2.2 以降でのみ使用できます。

- 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、VMware Cloud 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 --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
```

```
/opt/vmware/vcloud-director/bin/cell-management-tool reconfigure-database --database-
ssl true
```

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。キーストアのパスワードは、アプライアンスのデプロイ中に使用した root パスワードである場合があります。
- --database-password オプションは、https://appliance_eth0_ip:5480 にある、VMware Cloud Director アプライアンス管理ユーザー インターフェイスでアプライアンスをセットアップするとき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、[VMware Cloud Director アプライアンスに移行またはリストアすると VMware Cloud 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、VMware Cloud 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。『[VMware Cloud Director アプライアンスのデプロイと初期構成](#)』を参照してください。

- 7 新しいアプライアンスで、置き換えている元のアプライアンスと異なる IP アドレスを使用する場合は、VMware Cloud Director サーバ グループの前面に配置されたロード バランサの構成を更新して、新しいアプライアンスの IP アドレスを含める必要があります。
- 8 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、VMware Cloud 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、VMware Cloud Director Service Provider Admin Portal を開きます。
手順 7 でロード バランサの構成を更新した場合は、サーバ グループのパブリック アドレスを使用して Service Provider Admin Portal にアクセスする必要があります。
 - 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。
- 9 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 VMware Cloud Director 環境に属する切断されたセルを削除します。
 - a 上部ナビゲーション バーの [リソース] で [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。
- 10 リストア前のフェイルオーバー モードが `Automatic` だった場合、それを再度 `Automatic` に設定するには、VMware Cloud Director アプライアンス API を使用する必要があります。
- 11 リストア前に VMware Cloud Director アプライアンス FIPS モードがオンだった場合は、VMware Cloud Director アプライアンス API を使用して再設定する必要があります。
セルの FIPS モードが自動的にリストアされます。

VMware Cloud Director アプライアンスのフェイルオーバー モードの変更

デフォルトでは、VMware Cloud Director アプライアンスは手動フェイルオーバー モードになっていて、プライマリ データベース サービスに障害が発生した場合は、フェイルオーバー アクションを開始する必要があります。フェイルオーバー モードは、アプライアンス API を使用して自動に変更できます。

VMware Cloud Director 10.1 以降では、プライマリ データベース サービスに障害が発生した場合、VMware Cloud Director を有効にして、新しいプライマリへの自動フェイルオーバーを実行できます。[VMware Cloud Director アプライアンスの自動フェイルオーバー](#)を参照してください。

フェイルオーバー モードは、VMware Cloud Director アプライアンス API を使用して `automatic` または `manual` に設定されます。「[VMware Cloud Director アプライアンス API スキーマ リファレンス](#)」の「フェイルオーバー モード」セクションを参照してください。

自動フェイルオーバーが構成されたクラスタの場合、追加のセルを 1 つ以上デプロイした後に、アプライアンス API を使用してクラスタのフェイルオーバー モードを `automatic` にリセットする必要があります。クラスタのフェイルオーバー モードをリセットしないと、ノード間のフェイルオーバー モードが不整合な状態になります。

VMware Cloud 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 VMware Cloud Director データベースへのアクセスを有効にできます。

VMware Cloud 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 VMware Cloud 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 クライアントを使用して接続します。
- 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。

VMware Cloud 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。

前提条件

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 OVF プロパティの値を変更する必要があります。『vSphere 仮想マシン管理』ガイドの「vApp プロパティの構成」トピックを参照してください。

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、VMware Cloud Director のプロパティを変更します。
 - a VMware Cloud 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。

VMware Cloud Director アプライアンスでの FIPS モードの有効化または無効化

VMware Cloud Director アプライアンス バージョン 10.2.2 以降では、FIPS 140-2 認定の暗号化モジュールを使用して FIPS 対応モードで実行するように構成できます。

FIPS (Federal Information Processing Standard) 140-2 は、暗号化モジュールのセキュリティ要件を指定する、米国およびカナダの政府規格です。NIST Cryptographic Module Validation Program (CMVP) は、FIPS 140-2 規格に準拠した暗号化モジュールを検証します。

VMware Cloud Director FIPS サポートは、規制の厳しいさまざまな環境でのコンプライアンスとセキュリティのアクティビティを容易にすることを目的としています。VMware 製品における FIPS 140-2 のサポートの詳細については、<https://www.vmware.com/security/certifications/fips.html> を参照してください。

VMware Cloud Director では、FIPS 認定の暗号化はデフォルトで無効になっています。FIPS モードを有効にすることで、FIPS 140-2 認定の暗号化モジュールを使用し、FIPS 準拠モードで実行するように VMware Cloud Director が構成されます。

注： FIPS モードを有効にすると、ホスト名の逆引きも有効になります。

重要： FIPS モードを有効にした場合、vRealize Orchestrator との統合は動作しません。

VMware Cloud Director 10.2.2 で FIPS モードを有効にした場合は、SAML アサーションを暗号化できません。FIPS モードでない場合は、アサーション暗号化に制限はありません。

VMware Cloud Director は、次の FIPS 140-2 認定の暗号化モジュールを使用します。

- VMware の BC-FJA (Bouncy Castle FIPS Java API)、バージョン 1.0.2.1 : [Certificate #3673](#)
- VMware の OpenSSL FIPS オブジェクト モジュール、バージョン 2.0.20-vmw : [Certificate #3857](#)。

VMware Cloud Director はセル管理ツール (CMT) に付属のバンドルに含まれています。ただし、セル管理ツールは FIPS に準拠していません。

VMware Cloud Director アプライアンスを使用している場合に、アプライアンスを FIPS 準拠モードで実行するには、アプライアンス FIPS モードとセル FIPS モードの両方を管理する必要があります。

- アプライアンス FIPS モードは、基盤となるアプライアンス OS、組み込みデータベース、およびさまざまなシステム ライブラリのモードです。
- セル FIPS モードは、各アプライアンスで実行されている VMware Cloud Director セルのモードです。

Linux 上の VMware Cloud Director で FIPS モードを有効または無効にする方法については、[サーバ グループのセルでの FIPS モードの有効化](#)を参照してください。

前提条件

- メトリックの収集が有効になっている場合は、Cassandra 証明書が X.509 v3 証明書の標準に従っていて、必要なすべての拡張機能が含まれていることを確認します。Cassandra は、VMware Cloud Director が使用するのと同じ暗号化スイートを使用して構成する必要があります。許可された SSL 暗号の詳細については、[許可された SSL 暗号のリストの管理](#)を参照してください。
- VMware Cloud Director を vCenter Lookup Service から登録解除します。「VMware Cloud Director Service Provider Admin Portal Guide」の [vSphere サーボス構成](#)を参照してください。

手順

- 1 Service Provider Admin Portal の上部ナビゲーション バーで [管理] を選択します。
- 2 左側のパネルの [設定] で、[SSL] を選択します。
- 3 [有効化] をクリックします。
- 4 プロセスの開始を確定するには、[有効化] をクリックします。

構成が完了すると、VMware Cloud Director に「有効化が進行中 (セルの再起動を待機中)」というメッセージが表示され、手順 5 に進むことができます。手順 5 で API コマンドを実行すると、VMware Cloud Director アプライアンスによってセルは自動的に再起動されます。

- 5 アプライアンス FIPS モードをオンまたはオフにするには、VMware Cloud Director アプライアンス API を使用して `fips/{node_name}` の URL に PUT 要求を送信します。[VMware Cloud Director アプライアンス API](#) を参照してください。

注： PUT 要求を処理するマシンの `{node_name}` を使用する必要があります。

例：FIPS モードの有効化

要求：

```
PUT https://vcloud.example.com:5480/api/1.0.0/fips/{node_name}
Content-Type: application/json
...
{
  "applianceFips": "ON"
}
```

- 6 各アプライアンス（プライマリ、スタンバイなど）およびアプリケーションのタイプに、手順 5 を繰り返します。

次のステップ

セルの状態を確認するには、VMware Cloud Director アプライアンス管理ユーザー インターフェイスを使用します。[VMware Cloud Director アプライアンス FIPS モードの表示](#)を参照してください。

VMware Cloud Director アプライアンス FIPS モードの表示

VMware Cloud Director アプライアンス バージョン 10.2.2 以降は、FIPS 準拠モードで実行できます。アプライアンスとセルの FIPS モードを表示できます。

VMware Cloud Director アプライアンスを使用している場合に、VMware Cloud Director アプライアンスを FIPS 準拠モードで実行するには、アプライアンス FIPS モードとセル FIPS モードの両方を管理する必要があります。

- アプライアンス FIPS モードは、基盤となるアプライアンス OS、組み込みデータベース、およびさまざまなシステム ライブラリのモードです。
- セル FIPS モードは、各アプライアンスで実行されている VMware Cloud Director セルのモードです。

表 3-1. FIPS モードの状態

健全性	説明
	アプライアンスとセルの FIPS モードが一致します。どちらのモードもオンまたはオフです。
	セルの FIPS モードは、Pending restart の状態です。アプライアンス API を使用して、アプライアンスの FIPS モードを有効または無効にします。アプライアンスの FIPS モードを変更すると、VMware Cloud Director のセル サービスも自動的に再起動されます。
	VMware Cloud Director アプライアンスはセル FIPS モードを特定できません。アプライアンスで停止している VMware Cloud Director サービスがあると、セル FIPS モードが不確定になることがあります。

前提条件

VMware Cloud Director アプライアンスでの FIPS モードの有効化または無効化

手順

- 1 `https://primary_eth1_ip_address:5480` で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。
- 2 左側のパネルで [システム構成] を選択します。
- 3 各ノードのアプライアンスおよびセル FIPS モードのステータスを表示します。

VMware Cloud Director アプライアンス SNMP エージェントの構成

VMware Cloud Director 10.2.2 以降では、ポーリング要求を待機するように VMware Cloud Director アプライアンス SNMP エージェントを構成できます。

SNMP (Simple Network Management Protocol) は、ネットワーク要素を管理および監視するためのアプリケーション層プロトコルです。VMware Cloud Director アプライアンスには、GET、GETBULK、および GETNEXT 要求の受信と応答が可能な SNMP エージェントが含まれています。VMware Cloud Director アプライアンスの SNMP エージェントは、SNMP 標準に準拠しているすべての SNMP 管理サービスと互換性があります。SNMP v1、v2c、または v3 用にエージェントを構成できます。ただし、暗号化認証や暗号化などでセキュリティを強化できるのは、SNMP v3 のみです。

既存の Net-SNMP エージェントがある場合は、構成を開始する前に、次の点を考慮してください。

- VMware Cloud Director バージョン 10.2.2 以降へのアップグレード中に、Net-SNMP が削除されて、VMware-SNMP に置き換わります。
- `snmpd` サービスを開始および停止すると、VMware-SNMP によってポーリング元のポートがそれぞれ有効および無効になるため、Net-SNMP と連携する既存のファイアウォール ルールを削除する必要があります。

VMware Cloud Director アプライアンスの VMware-SNMP は、次の業界標準 MIB を介して使用できる標準の Linux OS 管理情報ベース (MIB) をサポートしています。

- SNMPv2-MIB
- RFC 3418IF-MIB
- RFC 2863IP-MIB
- RFC 4293IP-FORWARD-MIB
- RFC 4292UDP-MIB
- RFC 4113TCP-MIB
- RFC 4022ENTITY-MIB
- RFC 4133HOST-RESOURCES-MIB
- RFC 2790VMWARE-SYSTEM-MIB リビジョン 201008020000Z

SNMP エージェントのカスタム ポートの構成

VMware Cloud Director 10.2.2 以降では、ポーリングを行うように VMware Cloud Director SNMP エージェントを構成すると、SNMP 管理クライアント システムからの要求 (GET、GETNEXT、GETBULK 要求など) を待機し、応答できるようになります。

デフォルトで、組み込み SNMP エージェントは、UDP ポート 161 で管理システムからのポーリング要求を待機します。vicfg-snmp --port コマンドを使用して、代替ポートを構成できます。SNMP エージェントのポートと他のサービスのポート間の競合を回避するには、<https://ports.vmware.com/home/VMware-Cloud-Director> を参照してください。

前提条件

snmpd サービスを開始および停止すると、VMware-SNMP によってポーリング元のポートがそれぞれ有効および無効になるため、Net-SNMP と連携する既存のファイアウォール ルールを削除する必要があります。

手順

- 1 管理者権限を持つユーザーとして アプライアンス シェルにログインします。
- 2 次のコマンドを実行して、SNMP を無効にします。

```
vicfg-snmp --disable
```

- 3 SNMP エージェントがポーリング要求の待機に使用するポートを変更するには、次のコマンドを実行します。

```
vicfg-snmp --port port_number
```

SNMP v1 および v2c 用の VMware Cloud Director アプライアンスの構成

VMware Cloud Director 10.2.2 以降で VMware Cloud Director アプライアンスを SNMP 用に構成するには、SNMP エージェント用にコミュニティを 1 つ以上構成します。SNMP v1 および v2c 用に VMware Cloud Director SNMP エージェントを構成すると、エージェントでポーリングがサポートされます。

SNMP v1 および v2c では、コミュニティ文字列は 1 つ以上の管理対象オブジェクトを含む名前空間です。名前空間は認証のフォームとして機能することはできますが、通信は保護されません。通信を保護するには、SNMP v3 を使用します。

SNMP v1 および v2c メッセージを送受信するために VMware Cloud Director アプライアンス SNMP エージェントを有効にするには、エージェント用に 1 つ以上のコミュニティを構成する必要があります。SNMP コミュニティは、デバイスと管理システムのグループを定義します。同じコミュニティのメンバーであるデバイスおよび管理システムのみが、SNMP メッセージを交換できます。デバイスまたは管理システムは、複数のコミュニティのメンバーになることができます。

手順

- 1 管理者権限を持つユーザーとして アプライアンス シェルにログインします。
- 2 SNMP コミュニティを構成するには、vicfg-snmp -c コマンドを実行します。

たとえば、パブリック、東、および西のネットワーク オペレーション センターのコミュニティを構成するには、次のコマンドを実行します。

```
vicfg-snmp --communities public,eastnoc,westnoc
```

このコマンドでコミュニティを指定するたびに、指定した設定によって、以前の構成が上書きされます。複数のコミュニティを入力するには、区切り文字としてカンマを使用します。

3 次のコマンドを実行して、SNMP を有効にします。

```
vicfg-snmp --enable
```

SNMP v3 用の VMware Cloud Director アプライアンスの構成

VMware Cloud Director 10.2.2 以降では、SNMP v3 用に VMware Cloud Director アプライアンスを構成できます。SNMP v3 用に SNMP エージェントを構成すると、エージェントでポーリングがサポートされ、暗号化認証や暗号化などのセキュリティが強化されます。

SNMP v3 用に VMware Cloud Director アプライアンスを構成するには、次の 3 つの手順を実行します。

- 1 SNMP エンジン ID の構成
- 2 SNMP 認証およびプライバシー プロトコルの構成
- 3 SNMP ユーザーの構成

すべての SNMP v3 エージェントには、エージェントの一意の識別子として使用されるエンジン ID があります。エンジン ID は、SNMP v3 メッセージの認証と暗号化のためのローカライズされたキーを生成するときに、ハッシュ関数で使われます。SNMP エージェントを有効にする前にエンジン ID が指定されていない場合は、スタンドアロンの SNMP エージェントを有効にするときに、VMware Cloud Director エンジン ID が生成されます。

ユーザーの ID を確認するには、認証を使用します。プライバシーを使用すると、SNMP v3 メッセージを暗号化してデータの機密性を確保できます。プライバシー プロトコルは、セキュリティのためにコミュニティ文字列を使用する SNMP v1 および v2c より高いレベルのセキュリティを備えています。認証およびプライバシーは、いずれもオプションです。ただし、プライバシーを有効にする場合は、認証を有効にする必要があります。

認証プロトコルとプライバシー プロトコルのデフォルト値は「なし」です。

SNMP v3 情報にアクセスできるユーザーを、5 人まで設定できます。ユーザー名は、32 文字以下にする必要があります。ユーザーを構成するときに、ユーザーの認証パスワードとプライバシー パスワード、および SNMP エージェントのエンジン ID に基づいて、認証とプライバシーのハッシュ値を生成します。ユーザーを構成した後に、エンジン ID、認証プロトコル、またはプライバシー プロトコルを変更する場合は、ユーザーを無効にして再構成する必要があります。

前提条件

SNMP 認証およびプライバシー プロトコルを構成する場合は、構成する各ユーザーの認証パスワードとプライバシー パスワードを把握している必要があります。パスワードの長さは 8 文字以上である必要があります。

手順

- 1 管理者権限を持つユーザーとして アプライアンス シェルにログインします。
- 2 `vicfg-snmp --engineid` コマンドを実行してターゲットを構成します。

たとえば、次のコマンドを実行します。

```
vicfg-snmp --engineid 80001f8880167b18238d613d6000000000
```

ここで、80001f8880167b18238d613d6000000000 は ID（5 ～ 32 文字の 16 進文字列）です。

- 3 (オプション) 認証プロトコルを構成するには、`vicfg-snmp --authentication` コマンドを実行します。

たとえば、次のコマンドを実行します。

```
vicfg-snmp --authentication protocol
```

プロトコルは **なし** (認証しない場合)、**SHA1**、**SHA256**、**SHA384**、または **SHA512** にする必要があります。たとえば、認証プロトコルを SHA512 に設定する場合は、次のコマンドを実行する必要があります。

```
vicfg-snmp --authentication SHA512
```

- 4 (オプション) プライバシー プロトコルを構成するには、`vicfg-snmp --privacy` コマンドを実行します。たとえば、次のコマンドを実行します。

```
vicfg-snmp --privacy protocol
```

プロトコルは **なし** (プライバシーを使用しない場合)、**AES128**、**AES192**、または **AES256** にする必要があります。たとえば、プライバシー プロトコルを **AES128** に設定する場合は、次のコマンドを実行する必要があります。

```
vicfg-snmp --privacy AES128
```

- 5 認証、プライバシー、または両方を使用して、ユーザーの認証およびプライバシーのハッシュ値を生成する場合は、次のコマンドを実行します。

```
vicfg-snmp --hashkey authentication-password privacy-password
```

認証とプライバシーの設定に応じて、`authentication-password`、`privacy-password`、または両方を入力する必要があります。パスワードの長さは 8 文字以上である必要があります。SNMP クライアントを設定する際に必要になるため、`authentication-password` と `privacy-password` を書き留めます。コマンドの出力には、Authentication localized key と Privacy localized key の情報が含まれています。

- 6 次のコマンドを実行して、1 人以上のユーザーを構成します。

複数のユーザーを指定するには、ユーザーをカンマ区切りリストとして追加します。最大 5 人のユーザーを構成できます。

```
vicfg-snmp --users userid/authhash/privhash/security
```

コマンドのパラメータは次のとおりです。

パラメータ	説明
<code>userid</code>	ユーザー名で置き換えます。
<code>authhash</code>	認証のローカライズ キーで置き換えます。
<code>privhash</code>	プライバシーのローカライズ キーで置き換えます。
<code>model</code>	ユーザーに対して有効なセキュリティ レベルで置き換えます。 auth (認証のみ)、 priv (認証とプライバシー保護)、 none (認証もプライバシー保護もなし) のいずれかを指定できます。

たとえば、セキュリティなしでユーザーを構成する場合は、次のコマンドを実行できます。

```
vicfg-snmp --users vcd-snmp-user/-/-/none
```

認証ハッシュを使用してユーザーを構成する場合は、次のコマンドを実行します。

```
vicfg-snmp --users vcd-snmp-user/225e07958d3c6af615588db17d61986e69fb7a71/-/auth
```

認証ハッシュとプライバシー ハッシュを使用してユーザーを構成する場合は、次のコマンドを実行します。

```
vicfg-snmp --users vcd-snmp-user/225e07958d3c6af615588db17d61986e69fb7a71/  
da1057af05f67a25a09265a9a2bedb53/priv
```

- 7 (オプション) 1人以上のユーザーを削除する場合は、新しいユーザーの詳細を指定して手順 6 を繰り返します。

vicfg-snmp --users 再実行すると、以前のすべての設定がオーバーライドされます。

- 8 次のコマンドを実行して、SNMP を有効にします。

```
vicfg-snmp --enable
```

snmpwalk と VMware Cloud Director SNMP の併用

VMware Cloud Director 10.2.2 以降で、サブツリー内の各 OID またはノードに一意的なコマンド入力をせずに GETNEXT 要求のチェーンを作成するには、snmpwalk コマンドを実行します。

前提条件

- [SNMP v1 および v2c 用の VMware Cloud Director アプライアンスの構成](#) または [SNMP v3 用の VMware Cloud Director アプライアンスの構成](#) 用の VMware Cloud Director アプライアンスを構成します。

手順

- 1 ローカル マシンで、snmpwalk コマンドが導入されていることを確認し、必要に応じて導入します。
- 2 snmpwalk コマンドを実行します。

```
snmpwalk -v SNMP_version -l security_level -a authorization_protocol -A  
authorization_password -x privacy_protocol -X privacy_password -u username host_IP:port  
queried_MIB_OID
```

ここで、-l はセキュリティ レベルです (noAuthNoPriv、authNoPriv、または authPriv に設定可能)。snmpwalk コマンドのヘルプについては、-h を実行してください。

例: snmpwalk クエリ

sysDescr.0 MIB OID のサンプル クエリは次のとおりです。

```
snmpwalk -v 3 -l authPriv -a SHA512 -A myauthpassword -x AES128 -X myprivpassword -u vcd-snmp-  
user 192.168.100.187:10161 sysDescr.0
```

このコマンドは、次の出力を返します。

```
SNMPv2-MIB::sysDescr.0 = STRING: VMware-Cloud-Director-Appliance 10.2.2.5553 generic build
17709283 VMware, Inc x86_64
```

VMware Cloud Director アプライアンスの SNMP 設定のリセット

VMware Cloud Director 10.2.2 では、VMware Cloud Director アプライアンスの SNMP エージェントを構成できます。すべての SNMP 設定をクリアしてエージェントを無効にするには、アプライアンスの SNMP 設定をリセットします。

前提条件

[SNMP v1 および v2c 用の VMware Cloud Director アプライアンスの構成](#) または [SNMP v3 用の VMware Cloud Director アプライアンスの構成](#) 用の VMware Cloud Director アプライアンスを構成します。

手順

- 1 管理者権限を持つユーザーとして アプライアンス シェルにログインします。
- 2 すべての SNMP 設定をデフォルト値に戻し、SNMP エージェントを無効にするには、次のコマンドを実行します。

```
vicfg-snmp --reset
```

VMware Cloud Director アプライアンスの SNMP 設定の表示

VMware Cloud Director 10.2.2 以降では、UDP ポート、コミュニティ、V3 ユーザー、エンジン ID、認証およびプライバシー プロトコルなどの SNMP の設定を表示できます。

前提条件

[SNMP v1 および v2c 用の VMware Cloud Director アプライアンスの構成](#) または [SNMP v3 用の VMware Cloud Director アプライアンスの構成](#) 用の VMware Cloud Director アプライアンスを構成します。

手順

- 1 管理者権限を持つユーザーとして アプライアンス シェルにログインします。
- 2 SNMP の設定を表示するには、次のコマンドを実行します。

```
vicfg-snmp --show
```

例：vicfg-snmp --show のサンプル出力

サンプル出力には、認証ハッシュとプライバシー ハッシュを持つ V3 ユーザーに対して SNMP エージェントが有効になっていることが示されています。

```
Current SNMP agent setting
Enabled : true
UDP port : 161
V1/V2c Communities :
V1 Notification targets :
```

```

Notification filter oids:
V3 Notification targets :
V3 Users : vcd-snmp-user 225e07958d3c6af615588db17d61986e69fb7a71
da1057af05f67a25a09265a9a2bedb53 authPriv
Contact :
Location :
Engine ID : 80001f8880efbab0540a653e6000000000
Auth Protocol : usmHMACSHAAuthProtocol
Priv Protocol : usmAESCfb128PrivProtocol
Log level : warning
Process ID : 15828
Large Storage Support : False
Simple Application Names: False
INFO: listing complete.

```

VMware Cloud Director アプライアンスの DNS 設定の編集

デプロイ後に、VMware Cloud 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。

前提条件

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 OVF プロパティの値を変更する必要があります。『vSphere 仮想マシン管理』ガイドの「vApp プロパティの構成」トピックを参照してください。

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、VMware Cloud Director の DNS 設定を編集します。
 - a VMware Cloud 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。

VMware Cloud 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 VMware Cloud 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。

前提条件

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 OVF プロパティの値を変更する必要があります。『vSphere 仮想マシン管理』ガイドの「vApp プロパティの構成」トピックを参照してください。

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、VMware Cloud Director のスタティック ルートを編集します。
 - a VMware Cloud 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 VMware Cloud 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。

VMware Cloud Director アプライアンスでのスクリプトの設定

VMware Cloud 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。 VMware Cloud Director データベースへの外部アクセスの設定 を参照してください。

VMware Cloud Director アプライアンス証明書の更新

VMware Cloud 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 VMware Cloud Director セルの証明書を個別に更新する必要があります。

VMware Cloud Director アプライアンスは 2 セットの SSL 証明書を使用します。VMware Cloud Director サービスは、HTTPS およびコンソール プロキシの通信用に 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 VMware Cloud 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、VMware Cloud 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。
- FIPS モードが有効になっている場合、アプライアンスの root パスワードは 14 文字以上にする必要があります。[VMware Cloud Director アプライアンスの root パスワードの変更](#)を参照してください。

手順

- 1 VMware Cloud 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 VMware Cloud 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 データベースおよびアプライアンスの管理ユーザー インターフェイス用、または HTTPS およびコンソール プロキシ通信用の新しい自己署名証明書、データベース、およびアプライアンス管理ユーザー インターフェイスを生成します。

- 組み込みの PostgreSQL データベースと VMware Cloud Director アプライアンス管理ユーザー インターフェイス専用の自己署名証明書を生成して、以下を実行します。

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

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。

- 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 インターフェイスの証明書に加えて、VMware Cloud Director の HTTPS およびコンソール プロキシ通信用の新しい自己署名証明書を生成します。

- a 次のコマンドを実行します。

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

- b 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 VMware Cloud 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>
```

- c VMware Cloud Director サービスを再起動します。

```
service vmware-vcd start
```

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、4 で使用される VMware Cloud Director の HTTPS 通信およびコンソール プロキシ通信用の新しい自己署名証明書が生成されます。

結果

更新された自己署名証明書が、VMware Cloud 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 VMware Cloud Director セル上の VMware Cloud 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。

自己署名の組み込み PostgreSQL および VMware Cloud 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 VMware Cloud 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。

VMware Cloud 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。VMware Cloud Director アプライアンスは 2 セットの SSL 証明書を使用します。VMware Cloud Director サービスは、HTTPS およびコンソール プロキシの通信用に 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 VMware Cloud 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 VMware Cloud Director セル上の VMware Cloud 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。

VMware Cloud Director アプライアンス用の転送サーバ ストレージの置き換え

デプロイ後、VMware Cloud Director アプライアンス用の NFS 共有を変更できます。

手順

- 1 `vmware-vcd` サーバ グループ内のすべてのアプライアンスで、VMware Cloud Director サービス静止して停止します。

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

- 2 サーバ グループ内のすべてのアプライアンスで `appliance-sync.timer` サービスを停止します。

```
systemctl stop appliance-sync.timer
```

- 3 プライマリ アプライアンスで、古い NFS 共有から新しい NFS 共有にデータをコピーします。

- a 新しい NFS 共有のマウント ポイントを作成します。

```
mkdir /opt/vmware/vcloud-director/data/transfer-new/
```

- b 新しいマウント ポイントに新しい NFS サーバ共有をマウントします。

```
mount -t nfs Primary_appliance_IP_address:/data/transfer /opt/vmware/vcloud-director/data/transfer-new
```

- c 古い転送共有から新しい転送共有にファイルをコピーします。

注： ファイルのコピーにかかる時間は、転送フォルダ共有にキャッシュされているカタログ項目の数によって異なります。

```
cp -R /opt/vmware/vcloud-director/data/transfer/* /opt/vmware/vcloud-director/data/transfer-new/
```

- d ファイルが正常にコピーされたら、/opt/vmware/vcloud-director/data/transfer-new の内容を検証するか、次のコマンドを実行して、古い NFS 共有の内容が新しい NFS 共有に含まれていることを確認します。

```
diff -r --brief /opt/vmware/vcloud-director/data/transfer/ /opt/vmware/vcloud-director/data/transfer-new/
```

- e 一時的なマウント ポイントから新しい NFS 共有をアンマウントします。

```
umount /opt/vmware/vcloud-director/data/transfer-new/
```

- f 一時的なマウント ポイントを削除します。

```
rmdir /opt/vmware/vcloud-director/data/transfer-new/
```

- 4 /etc/fstab ファイルを更新して、NFS 行を新しい NFS サーバへのパスに置き換えます。

```
Primary_appliance_IP_address:/data/transfer_appliance /opt/vmware/vcloud-director/data/transfer/ nfs defaults 0 0
```

- 5 古い NFS 共有をアンマウントします。

```
umount /opt/vmware/vcloud-director/data/transfer/
```

- 6 新しい NFS 共有をマウントします。

```
mount -a
```

- 7 mount コマンドの出力にマウントした NFS 共有が表示されていることを検証して、NFS 共有が正常にマウントされたことを確認します。

- 8 次のコマンドを使用して、転送ディレクトリの所有権を root から vcloud に変更します。

```
chown -R vcloud:vcloud /opt/vmware/vcloud-director/data/transfer
```

- 9 appliance-sync.timer サービスを再起動します。

```
systemctl start appliance-sync.timer
```

- 10 サーバ グループ内のすべてのノードで手順 4 ～ 9 を繰り返します。

- 11 1 ノードずつ vmware-vcd サービスを再起動します。

```
systemctl start vmware-vcd
```

- 12 サーバ グループ内のすべてのノードで vmware-vcd が正しく動作することを確認します。

VMware Cloud 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

VMware Cloud 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。

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 ディスクと同じにする必要があります。

前提条件

- VMware Cloud 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、[VMware Cloud Director アプライアンス クラスターの健全性とフェイルオーバー モードの表示](#)を参照してください。
- VMware Cloud 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 アプライアンス ノードの OS に変更を適用します。

- a VMware Cloud 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、次のスクリプトを実行します。

```
/opt/vmware/appliance/bin/db_diskresize.sh
```

- 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なければ、データベースを含む各ノードに対してこの手順を繰り返します。

VMware Cloud Director アプライアンスでの PostgreSQL 設定の変更

VMware Cloud 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 ファイルを変更しないでください。クラスタの操作でこのファイルを定期的に上書きする必要があり、変更は維持されないためです。

手順

- 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。
- ユーザーを postgres に変更します。

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

- 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';"
```

- 変更する構成パラメータごとに [手順 3](#) を繰り返します。
- 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
```

- 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。

- 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/
```

- 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
```

- 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。

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。

VMware Cloud Director アプライアンス API の詳細については、[VMware Cloud Director アプライアンス API](#) のドキュメントを参照してください。

通常のシステム運用中にセルを登録解除することができます。

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。

手順

- 1 登録解除するスタンバイ ノードの名前を確認するには、VMware Cloud Director アプライアンス API の `NODES` メソッドを実行します。
- 2 ほかのいずれかのノードから、VMware Cloud Director アプライアンス API の `UNREGISTER` メソッドを実行します。

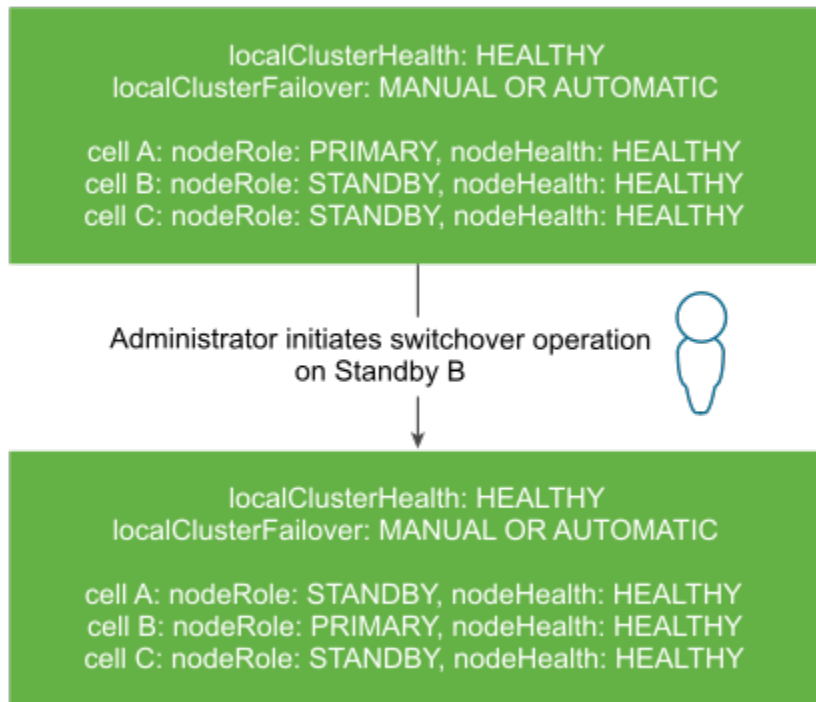
ここで、`node-name` は、削除するスタンバイ アプライアンスの名前です。
- 3 登録解除されたスタンバイ ノードがデータベース高可用性クラスタに含まれなくなったことを確認するには、API の `NODES` メソッドを実行します。

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

VMware Cloud Director アプライアンスの管理ユーザー インターフェイスを使用して、データベース高可用性クラスタ内のセルのロールを切り替え、別のセルをプライマリとして昇格させることができます。

プライマリおよびスタンバイ セルのロールは、VMware Cloud Director アプライアンス管理ユーザー インターフェイスまたは VMware Cloud Director アプライアンス API を使用して切り替えることができます。この手順では、管理ユーザー インターフェイスを使用して切り替えを行う手順について説明します。

図 3-3. プライマリ セルとスタンバイ セルの切り替え

**前提条件**

- 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。[VMware Cloud Director アプライアンス クラスタの健全性とフェイルオーバー モードの表示](#)を参照してください。

手順

- 1 サーバ グループに属するすべての VMware Cloud Director セルのアクティビティを停止するか、セルをメンテナンス モードにします。
この切り替えにより、VMware Cloud Director データベースは 30 ～ 60 秒間使用できなくなります。タスクの予期しない失敗を回避するために、クラスタ内のすべてのセルのアクティビティを停止する必要があります。
- 2 https://primary_eth1_ip_address:5480 で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。
- 3 左側のパネルで [組み込みデータベース可用性] を選択します。
セルの名前、ロール、ステータス、およびスタンバイ セルがフォローしているセルの名前を表示できます。
- 4 クラスタの健全性が `Healthy` であることを確認します。
- 5 プライマリとして昇格させるセルの [切り替え] ボタンをクリックして、切り替えを確認します。
- 6 切り替えタスクが完了したら、スケジューラを再起動するか、クラスタ内のセルのメンテナンス モードを無効にします。

MQTT クライアントを使用したイベント、タスク、およびメトリックへのサブスクリプション

MQTT クライアントを使用して、VMware Cloud Director のイベントおよびタスクに関するメッセージをサブスクリプションすることができます。

MQTT は、軽量でバイナリ形式のメッセージ転送プロトコルです。VMware Cloud Director は MQTT を使用して、MQTT クライアントを使用してサブスクリプションできるイベントおよびタスクに関する情報を公開します。

MQTT メッセージは MQTT ブローカを通過しますが、クライアントがオンラインでないとき、MQTT ブローカはメッセージを保存することもできます。

VMware Cloud Director 10.2.2 以降では、MQTT クライアントを使用してメトリックにサブスクリプションできます。

前提条件

- WebSocket をサポートする MQTT クライアントがあることを確認します。
- WebSocket にアップグレードされた要求にヘッダーを追加できることを確認します。
- メトリックにサブスクリプションする場合は、メトリックの収集を構成し、メトリックの公開を有効にします。 [メトリックの収集と公開の構成](#)を参照してください。

手順

- 1 OpenAPI エンドポイントを使用して VMware Cloud Director にログインします。
- 2 WebSocket 接続を確立するには、Sec-WebSocket-Protocol プロパティを `mqtt` に設定し、クライアントが `/messaging/mqtt` パスに接続するように設定し、認証ヘッダーを追加して、標準の MQTT 接続フローを実行します。

VMware Cloud Director に対する標準のログイン要求から JWT トークンを受け取ります。ユーザー名とパスワードは空のままにすることができます。

```
Sec-WebSocket-Protocol: mqtt
```

```
Authorization: Bearer {JWT_token}
```

- 3 接続が正常に確立されたら、MQTT クライアントを通じてトピックをサブスクリプションします。

```
publish/{user_org_id}/{user_id}
```

```
publish/debd63a0-6eae-11ea-8c7b-0050561776be/d19fd8ff-6eae-11ea-bb42-0050561776c8
```

組織管理者は、ワイルドカードを使用してすべての組織のトピックにアクセスできます。

```
publish/{user_org_id}/+
```

システム管理者は、ワイルドカードを使用してすべてのトピックにアクセスできます。

```
publish/#
```

4 （オプション） VMware Cloud Director 10.2.2 以降では、メトリックにサブスクライブします。

```
metrics/{org_id}/{vApp_id}
```

メトリックのトピックにアクセスできるのは、システム管理者のみです。

自動スケール グループ

VMware Cloud Director 10.2.2 以降では、テナント ユーザーに、現在の CPU およびメモリの使用量に応じて、アプリケーションを自動スケールする許可を与えることができます。

CPU およびメモリの使用量について事前定義された基準に応じて、テナントは VMware Cloud Director を使用して、選択したスケール グループ内の仮想マシンの数を自動的に増減できます。テナントがアプリケーションを自動スケールできるようにするには、自動スケール ソリューションへのアクセス権を構成、公開、および付与する必要があります。

同じアプリケーションを実行するように構成したサーバの負荷を分散させるには、VMware NSX Advanced Load Balancer (Avi Networks) を使用します。

自動スケール プラグインの構成と公開

テナントへのアクセス権を付与する前に、自動スケール グループ ソリューションを構成する必要があります。自動スケールは VMware Cloud Director 10.2.2 以降で使用できます。

- 1 クラスタ内のいずれかのセルの OS に root として直接、または SSH クライアントを使用してログインします。
- 2 Cassandra データベースでメトリック収集を設定して、メトリック データの収集を有効にするか、メトリック データの永続性なしでメトリックを収集します。

- [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](#)
- データの永続性なしでメトリック データを収集するには、次のコマンドを実行します。

```
/opt/vmware/vcloud-director/bin/cell-management-tool manage-config -n
statsFeeder.metrics.collect.only -v true
```

- 3 メトリックの公開を有効にします。

```
/opt/vmware/vcloud-director/bin/cell-management-tool manage-config -n
statsFeeder.metrics.publishing.enabled -v true
```

- 4 /tmp フォルダ内に、次の内容を含む metrics.groovy ファイルを作成します。

```
configuration {
    metric("cpu.ready.summation") {
        currentInterval=20
        historicInterval=20
        entity="VM"
        instance=""
    }
}
```

```

        minReportingInterval=300
        aggregator="AVERAGE"
    }
}

```

- 5 ファイルをインポートします。

```

$VCLLOUD_HOME/bin/cell-management-tool configure-metrics --metrics-config /tmp/
metrics.groovy

```

- 6 以前に Cassandra を構成している場合は、適切なノード アドレス、データベース認証の詳細、ポートおよびメトリックの有効日数を指定して Cassandra スキーマを更新します。

```

$VCLLOUD_HOME/bin/cell-management-tool cassandra -configure -cluster-nodes
nodes_IP_addresses -username cassandra -password cassandra_password -port port_number -ttl
TTL_days -update-schema

```

- 7 CA 署名付き証明書を使用してセルを実行する場合、自動スケール有効にするには、次のコマンドを実行します。

```

$VCLLOUD_HOME/bin/cell-management-tool configure-autoscale --set enabled=true
$VCLLOUD_HOME/bin/cell-management-tool configure-autoscale --set username=<username>
$VCLLOUD_HOME/bin/cell-management-tool configure-autoscale --encrypt --set
password=<password>

```

ターミナルからコマンドを実行する場合は、バックスラッシュ (\) 記号を使用して特殊文字をエスケープします。

- 8 セルを再起動します。

```

service vmware-vcd restart

```

9 自動スケール権限バンドルの公開

自動スケール権限バンドルの公開

テナントがアプリケーションを自動スケールする場合は、システム内の 1 つ以上の組織に権限バンドルを公開する必要があります。自動スケールは VMware Cloud Director 10.2.2 以降で使用できます。

前提条件

自動スケール プラグインの構成と公開

手順

- 1 上部ナビゲーション バーで [管理] を選択します。
- 2 左側のパネルの [テナント アクセス コントロール] で、[権限バンドル] を選択します。
- 3 自動スケールへのアクセス権を付与するテナント組織に、レガシー権限バンドルがないことを確認します。
- 4 vmware:scalegroup Entitlement バンドルを選択して、[公開] をクリックします。

5 バンドルを公開するには：

- a [テナントに公開] を選択します。
- b ロールを公開する組織を選択します。
 - バンドルをシステム内のすべての既存の組織および新規に作成された組織に公開する場合は、[すべてのテナントに公開] を選択します。
 - システム内の特定の組織にバンドルを公開する場合は、組織を個別に選択します。

6 [保存] をクリックします。

次のステップ

自動スケールを使用するテナント ロールに必要な VMWARE:SCALEGROUP 権限を追加します。「VMware Cloud Director Service Provider Admin Portal Guide」の[グローバル テナント ロールの表示と編集](#)を参照してください。

VMware Cloud Director アプライアンス データベース クラスタの健全性の監視

VMware Cloud Director アプライアンス クラスタを監視するには、VMware Cloud Director アプライアンス 管理ユーザー インターフェイス、アプライアンス API、または repmgr オープンソース ツール スイートを使用します。

VMware Cloud Director アプライアンス管理ユーザー インターフェイスを使用して、アプライアンスのフェイルオーバー モードを表示することもできます。フェイルオーバー モードは、プライマリ データベースに障害が発生した場合に VMware Cloud Director がデータベースのフェイルオーバーを自動的にトリガーするか、システム管理者が手動でフェイルオーバーを開始する必要があるかを示します。

ノード間でフェイルオーバー モードに一貫性がない場合は、フェイルオーバー モードは Indeterminate です。

Indeterminate モードでは、元のプライマリ セルをフォローするノード間でクラスタの状態が不整合になる可能性があります。問題を診断して、状態を手動で修正する必要があります。

VMware Cloud Director アプライアンス クラスタの健全性とフェイルオーバー モードの表示

VMware Cloud Director アプライアンス管理ユーザー インターフェイスを使用して、クラスタのステータスを監視できます。

VMware Cloud Director アプライアンス管理ユーザー インターフェイスまたは VMware Cloud Director アプライアンス API を使用して、クラスタ内のセルの名前、セルのロール、セルのステータス、スタンバイ セルがフォローしているセルの名前、およびクラスタ フェイルオーバー モードを表示できます。この手順では、管理ユーザー インターフェイスでアプライアンス クラスタの健全性を監視する手順について説明します。

手順

- 1 https://primary_eth1_ip_address:5480 で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。

2 左側のパネルで [組み込みデータベース可用性] を選択します。

ノードの短い DNS 名、そのロール、ステータス、アップストリーム ノード（現在のプライマリ）の名前、およびノードで使用可能なアクションを表示できます。

[フォロー中] 列のホスト名の前に付いている感嘆符 (?) は、現在のプライマリが到達不可能であることを示しています。ホスト名の前に付いている感嘆符 (!) は、現在のプライマリのメタデータが更新されておらず、誤っている可能性があること、またはノードが現在のプライマリに接続されていないことを示しています。この問題は、長時間のダウンタイム後にノードを再起動した場合に発生することがあります。ノードをプライマリに接続できない場合は、ノードを登録解除し、新しいスタンバイに置き換える必要があります。

3 クラスタの健全性を表示します。

クラスタの健全性ステータス	説明
健全	クラスタは良好な状態です。プライマリ セルと両方のスタンバイセルが、オンラインで動作しています。 VMware Cloud Director ユーザー インターフェイスと API は機能しています。
劣化	クラスタは劣化状態です。プライマリ セルとスタンバイ セルの 1 つがオンラインで動作していますが、その他のスタンバイ セルは機能していません。プライマリ データベースはこの状態でも機能しますが、操作可能なセルのいずれかで別のデータベース障害が発生した場合、プライマリは機能しなくなります。クラスタを <i>Healthy</i> な状態にリストアするために、機能していないスタンバイ セルを機能している新しいスタンバイ セルに速やかに置き換える必要があります。 VMware Cloud Director ユーザー インターフェイスと API は機能しています。
No_Active_Primary	操作可能なプライマリ データベースがありません。操作可能なスタンバイ セルが 2 つある場合は、そのうちの 1 つを昇格させて新しいプライマリ セルにする必要があります。環境に 2 つの操作可能なスタンバイ セルがない場合は、問題を診断して、状態を手動で修正する必要があります。 VMware Cloud Director ユーザー インターフェイスと API は使用できません。
Read_Only_Primary	オンラインのプライマリ データベースはありますが、この環境には操作可能なスタンバイ セルがないため、 <i>Read_Only</i> の状態です。2 つの新しいスタンバイ セルをデプロイする必要があります。 VMware Cloud Director ユーザー インターフェイスと API は使用できません。

クラスタの健全性ステータス	説明
Critical_Problem	クラスタが不整合な状態です。たとえば、複数のプライマリ セルがオンラインである場合や、スタンバイ セルが誤ったプライマリ セルをフォローしている場合です。問題を診断して、状態を手動で修正する必要があります。 この状態は、VMware Cloud Director ユーザー インターフェイスおよび API の可用性に影響する可能性があります。
SSH_Problem	SSH 問題は、postgres ユーザーが SSH を使用してピア データベース ノードに接続できないことを示しています。この問題は重大であるため、可能な限り早く修正する必要があります。 クラスタの健全性で SSH の問題が示されている場合 を参照してください。 VMware Cloud Director ユーザー インターフェイスおよび API が完全には機能しない可能性があります。

4 アプライアンスのフェイルオーバー モードを表示します。

フェイルオーバー モード	説明
自動	プライマリ データベースの障害が発生すると、VMware Cloud Director によってデータベースのフェイルオーバーが自動的にトリガーされます。
手動	プライマリ データベースの障害が発生した場合は、VMware Cloud Director アプライアンス管理ユーザー インターフェイス、またはフェイルオーバー API を使用して、データベースのフェイルオーバーを開始する必要があります。
不明	クラスタのすべてのノード間で、フェイルオーバー モードが不整合な状態です。問題を診断して、状態を修正する必要があります。 VMware Cloud Director アプライアンス API を使用して、FailoverMode を Manual または Automatic にリセットします。『VMware Cloud Director アプライアンス API スキーマ リファレンス』の「Failovermode」を参照してください。

VMware Cloud Director アプライアンス サービス ステータスの表示

VMware Cloud Director アプライアンス管理ユーザー インターフェイスを使用して、VMware Cloud Director アプライアンス サービスのステータスを監視できます。

[サービス] タブで、プライマリ アプライアンスとスタンバイ アプライアンスの vmware-vcd、vpostgres、appliance-sync.timer サービス、およびアプリケーション セルの vmware-vcd および appliance-sync.timer サービスを監視できます。

appliance-sync.timer サービスは appliance-sync.service を定期的に行うことで、データベース HA クラスタまたは VMware Cloud Director サーバ グループ内のすべてのノード間で関連情報を共有します。appliance-sync.service は、アプライアンス グループ内のアプライアンスの構成ファイルの読み取りと書き込みを行うことによって、VMware Cloud Director アプライアンスの機能に必要なファイルを定期的を確認し、同期します。タイマーの健全な状態は、waiting と running です。

手順

- 1 `https://primary_eth1_ip_address:5480` で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。
- 2 左側のパネルで、[サービス] タブを選択します。
- 3 VMware Cloud Director サービスのステータスを確認します。

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

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 つのサーバに対応し、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
```

プライマリのシステム出力には、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。以下にその例を挙げます。

```

Node "bos1-vcloud-static-161-5":
  PostgreSQL version: 10.9
  Total data size: 81 MB
  Conninfo: host=172.18.36.193 user=repmgr dbname=repmgr connect_timeout=2
  Role: primary
  WAL archiving: off
  Archive command: (none)
  Replication connections: 2 (of maximal 10)
  Replication slots: 0 physical (of maximal 10; 0 missing)
  Replication lag: n/a

```

スタンバイ ノードのシステム出力には、ノード、PostgreSQL のバージョン、レプリケーションの詳細、およびアップストリーム ノードに関する情報が示されます。以下にその例を挙げます。

```
Node "bos1-vcloud-static-161-49":
  PostgreSQL version: 10.9
  Total data size: 83 MB
  Conninfo: host=172.18.36.191 user=repmgr dbname=repmgr connect_timeout=2
  Role: standby
  WAL archiving: off
  Archive command: (none)
  Replication connections: 0 (of maximal 10)
  Replication slots: 0 physical (of maximal 10; 0 missing)
  Upstream node: bos1-vcloud-static-161-48 (ID: 683)
  Replication lag: 0 seconds
  Last received LSN: 2/D863B4E0
  Last replayed LSN: 2/D863B4E0
```

- 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>select* from pg_stat_replication;</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>

VMware Cloud Director サービスのステータスの確認

VMware Cloud Director アプライアンスの管理ユーザー インターフェイスを使用して、ログインしているセルの VMware Cloud Director サービスのステータスを表示できます。

手順

- 1 `https://primary_eth1_ip_address:5480` で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。
- 2 サービスのステータスを表示するには、左側のパネルで [サービス] を選択します。

VMware Cloud Director アプライアンスが正常に動作している場合は、vmware-vcd および vpostgres サービスが実行されています。

次のステップ

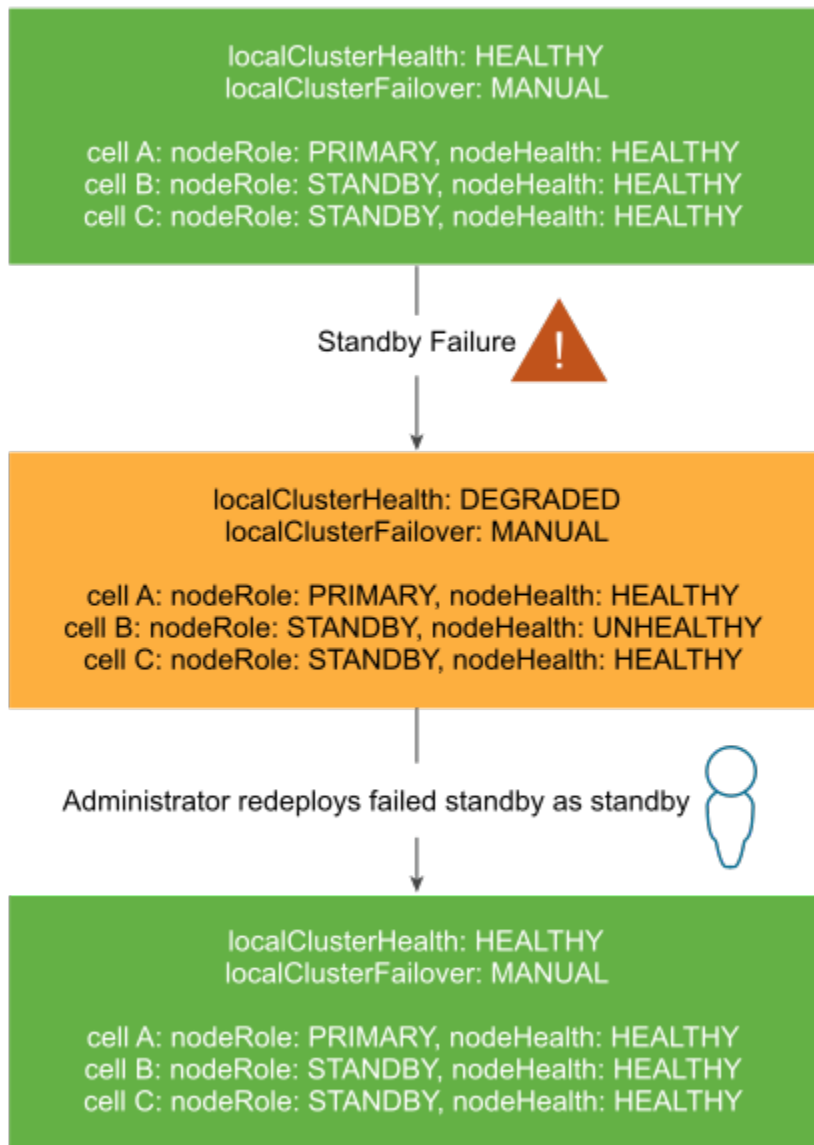
デバッグのために `repmgrd` サービスのステータスを確認する必要がある場合は、VMware Cloud Director アプライアンス API を使用する必要があります。

VMware Cloud Director アプライアンス データベース クラスタのリカバリ

データベース、または VMware Cloud Director ノードのいずれかで障害が発生した場合は、データベース クラスタをリカバリすることができます。

データベース高可用性クラスタ内のセルで障害が発生した場合、クラスタの健全性ステータスに、障害の内容と問題の解決方法が示されます。たとえば、Degraded クラスタの健全性は、スタンバイ セルで障害が発生したことを示します。システム管理者は、障害が発生したセルを再デプロイする必要があります。

図 3-4. スタンバイ セルの障害からのリカバリ



データベース高可用性クラスタ内のプライマリ セルに障害が発生すると、クラスタの健全性は `No_Active_Primary` に変更されます。これは、システム管理者が障害が発生したプライマリ セルを修復する必要があることを示します。

高可用性クラスタのプライマリ セル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、VMware Cloud 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 セルが新しいプライマリ セルになる必要があり、また、新しいスタンバイをデプロイする必要があります。障害モードに応じて、VMware Cloud Director アプライアンスでスタンバイ セルが新しいプライマリ として自動的に昇格されるか、または手動で昇格する必要があります。

VMware Cloud Director アプライアンスのフェイルオーバー モードに応じて、プライマリ セルの障害からリカバリするための 2 つの異なるワークフローがあります。これら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。

手動フェイルオーバー モードのリカバリ ワークフロー

プライマリ セルの状態が Not reachable または Failed で、2 つのスタンバイ セルの状態が Running である場合、障害からリカバリするには、アプライアンス HTML5 ユーザー インターフェイスと VMware Cloud Director アプライアンス API を使用します。

クラスタ内のセルの状態を表示するには、[VMware Cloud Director アプライアンス クラスタの健全性とフェイルオーバー モードの表示](#) を参照してください。

- 1 可能であれば、セル管理ツールを使用して VMware Cloud 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 <sysadmin user> 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 スタンバイ セルを昇格させて新しいプライマリにします。

- a 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)。
- b 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。

管理ユーザー インターフェイスには、primary ロールを持つ 2 つのセルが表示されます。元のプライマリは failed ステータス、新しいプライマリは running ステータスとなっています。クラスタの健全性は Degraded です。

- 4 障害のあるプライマリ以外のセルからアプライアンス API Unregister メソッドを使用して、repmgr 高可用性クラスタから失敗したプライマリ アプライアンスを削除します。[VMware Cloud Director アプライアンス API](#) のドキュメントを参照してください。
- 5 障害のあるプライマリ アプライアンスを VMware Cloud Director サーバ グループから削除します。
 - a Service Provider Admin Portal に管理者としてログインします。
 - b 上部ナビゲーション バーの [リソース] で [クラウド リソース] を選択します。
 - c 左側のパネルで [クラウド セル] をクリックします。
 - d 無効なセルを選択し、[登録解除] をクリックします。
- 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、vSphere Client を使用してこのアプライアンスを削除します。
- 7 新しいスタンバイ アプライアンスをデプロイします。[VMware Cloud 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 VMware Cloud 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。

- 8 リストア前に VMware Cloud Director アプライアンス FIPS モードがオンだった場合は、VMware Cloud Director アプライアンス API を使用して再設定する必要があります。

セルの FIPS モードが自動的にリストアされます。

自動フェイルオーバー モードのリカバリ

プライマリが Failed 状態の場合、VMware Cloud Director はスタンバイ セルを新しい実行中のプライマリとして自動的に昇格させます。ただし、実行中のスタンバイ セルが 1 つのみのため、クラスタは Degraded 状態になっています。HTML5 ユーザー インターフェイスと VMware Cloud Director アプライアンス API を使用して、この障害からリカバリできます。

クラスタ内のセルの状態を表示するには、[VMware Cloud Director アプライアンス クラスタの健全性とフェイルオーバー モードの表示](#) を参照してください。

- 1 可能であれば、セル管理ツールを使用して VMware Cloud 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 <sysadmin user> 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。

管理ユーザー インターフェイスには、primary ロールを持つ 2 つのセルが表示されます。元のプライマリは failed ステータス、新しいプライマリは running ステータスとなっています。クラスタの健全性は Degraded です。

- 3 障害のあるプライマリ以外のセルからアプライアンス API Unregister メソッドを使用して、repmgr 高可用性クラスタから失敗したプライマリ アプライアンスを削除します。[VMware Cloud Director アプライアンス API](#) のドキュメントを参照してください。
- 4 障害のあるプライマリ アプライアンスを VMware Cloud Director サーバ グループから削除します。
 - a Service Provider Admin Portal に管理者としてログインします。
 - b 上部ナビゲーション バーの [リソース] で [クラウド リソース] を選択します。
 - c 左側のパネルで [クラウド セル] をクリックします。
 - d 無効なセルを選択し、[登録解除] をクリックします。
- 5 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するか、vSphere Client を使用してこのアプライアンスを削除します。
- 6 新しいスタンバイ アプライアンスをデプロイします。[VMware Cloud 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 VMware Cloud 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。
- 7 障害のあるプライマリ セル以外のセルから、アプライアンス API Failover メソッドを使用してクラスタ フェイルオーバー モードを Automatic にリセットします。[VMware Cloud Director アプライアンス API](#) のドキュメントを参照してください。
- 8 リストア前に VMware Cloud Director アプライアンス FIPS モードがオンだった場合は、VMware Cloud Director アプライアンス API を使用して再設定する必要があります。

セルの FIPS モードが自動的にリストアされます。

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 `Not reachable` 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、[VMware Cloud Director アプライアンス クラスタの健全性とフェイルオーバー モードの表示](#) 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 VMware Cloud 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 障害のあるスタンバイ セル以外のセルからアプライアンス API `Unregister` メソッドを使用して、`repmgr` 高可用性クラスタから失敗したスタンバイ セルを削除します。[VMware Cloud Director アプライアンス API](#) のドキュメントを参照してください。
- 4 Service Provider Admin Portal を使用して、障害のあるスタンバイ アプライアンスを VMware Cloud Director サーバ グループから削除します。
 - a 上部ナビゲーション バーの [リソース] で [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。
- 5 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。
- 6 新しいスタンバイ アプライアンスをデプロイします。[VMware Cloud 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 VMware Cloud 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。

- 7 クラスタ フェイルオーバー モードを `Automatic` にリセットするには、障害のあるスタンバイ セル以外のセルからアプライアンス API `Failover` メソッドを使用します。[VMware Cloud Director アプライアンス API](#) のドキュメントを参照してください。

自動フェイルオーバー モードの詳細については、[VMware Cloud Director アプライアンスの自動フェイルオーバー](#) を参照してください。

- 8 リストア前に VMware Cloud Director アプライアンス FIPS モードがオンだった場合は、VMware Cloud Director アプライアンス API を使用して再設定する必要があります。

セルの FIPS モードが自動的にリストアされます。

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 セルまたはスタンバイ セルの登録解除

データベース高可用性クラスタのプライマリ ノードまたはスタンバイ ノードで障害が発生した場合は、VMware Cloud Director API を使用して障害が発生した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 データの不整合な状態を回避することができます。

VMware Cloud Director API の使用方法の詳細については、<https://developer.vmware.com/> にある VMware Cloud Director Appliance API ドキュメントの「UNREGISTER API メソッド」を参照してください。

前提条件

- 登録解除するノードが非アクティブになっていることを確認し、そのノードの名前を書き留めます。セルのステータスと、スタンバイ セルに適用されるセルの名前については、[VMware Cloud Director アプライアンス クラスタの健全性とフェイルオーバー モードの表示](#)を参照してください。
- プライマリ ノードを登録解除する場合は、障害が発生したプライマリが非アクティブで、後続のスタンバイ ノードがないことを確認し、新しいプライマリを昇格させます。

手順

- ◆ 非アクティブ ノードを削除するには、コマンドを実行するアクティブ ノードで削除要求を行います。

```
DELETE https://<Active _Node_FQDN>:5480/api/1.0.0/nodes/<Inactive_Node_Name>
```

アプライアンスのトラブルシューティング

VMware Cloud 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 VMware Cloud Director ログを収集できます。

VMware Cloud 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。

VMware Cloud Director アプライアンスのログ ファイルの調査

VMware Cloud 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 VMware Cloud 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。
- 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 VMware Cloud Director のセルの起動に失敗する

VMware Cloud Director アプライアンスが正常にデプロイされても、VMware Cloud 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、VMware Cloud 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、VMware Cloud 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。

注: クラスタが自動フェイルオーバー用に構成されている場合は、追加セルをデプロイした後、アプライアンス API を使用して、そのフェイルオーバー モードを `Automatic` に設定する必要があります。「[VMware Cloud Director アプライアンス API](#)」を参照してください。新しいセルのデフォルトのフェイルオーバー モードは `Manual` です。クラスタのノード間でフェイルオーバー モードが不整合な状態の場合は、クラスタのフェイルオーバー モードは `Indeterminate` です。Indeterminate モードでは、元のプライマリ セルをフォローするノード間でクラスタの状態が不整合になる可能性があります。クラスタのフェイルオーバー モードを表示するには、[VMware Cloud Director アプライアンス クラスタの健全性とフェイルオーバー モードの表示](#)を参照してください。

解決方法

- 1 VMware Cloud 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。
- 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。

アプライアンスの初期構成中に NFS 検証が失敗した後のリカバリ

VMware Cloud Director アプライアンスの初期構成中に共有ストレージの検証に失敗すると、問題の修正に使用できるエラー メッセージが表示されます。

問題

VMware Cloud Director アプライアンスのデプロイ中に、NFS 共有を参照するエラー メッセージが表示されます。

原因

VMware Cloud Director の転送サーバ ストレージの準備ができていない場合は、デプロイ中に NFS 検証が失敗します。

解決方法

バージョン	エラー	アクション
10.2	<code>/opt/vmware/vcloud-director/data/transfer/xyz</code> は UID が 999 の不明なユーザーによって所有されています。予期される UID は 1003 です	NFS サーバで vcloud ユーザーのユーザー ID の設定を確認します。vcloud ユーザー ID の値は、NFS サーバとアプライアンスで同じである必要があります。
10.2	<code>/opt/vmware/vcloud-director/data/transfer/xyz</code> は GID が 999 の不明なユーザーによって所有されています。予期される GID は 1002 です	NFS サーバで vcloud ユーザーのグループ ID の設定を確認します。vcloud ユーザー ID の値は、NFS サーバとアプライアンスで同じである必要があります。
10.2	転送共有の実行時にファイルを使用できません	マウントされた NFS 共有にアプライアンスが書き込みを実行できない理由を特定します。書き込みができない理由を確認するには、別の Linux マシンを使用して NFS 共有をマウントします。
10.2	<code>/usr/bin/mount -t nfs 10.150.170.3:/data/transfer /opt/vmware/vcloud-director/data/nfs-test</code> の実行中にタイムアウトが発生しました。期間: 5 秒	指定された NFS 共有をこのアプライアンスが 5 秒以内にマウントできない理由を特定します。NFS 共有を適切なタイミングでマウントできるかどうかを確認するには、別の Linux マシンを使用してマウントします。または、この NFS 共有の NFS サーバエクスポート設定を確認します。
10.2	<code>/usr/bin/mount -t nfs 10.150.170.3:/data/transfer /opt/vmware/vcloud-director/data/nfs-test</code> の実行中にエラーが発生しました。	このアプライアンスが指定された NFS 共有をマウントできない理由を特定します。NFS 共有をマウントできないかどうかを確認するには、別の Linux マシンを使用してマウントします。または、この NFS 共有の NFS サーバエクスポート設定を確認します。
10.2	転送共有ディレクトリが存在しません: <code>/opt/vmware/vcloud-director/data/transfer</code>	転送共有ディレクトリまたはマウント ポイントが存在しません。該当するディレクトリを作成します。

バージョン	エラー	アクション
10.2	操作: touch xyz の実行中に /opt/vmware/vcloud-director/data/transfer/xyz ファイルに予期しない権限が見つかりました。予期された権限: root root 644。検出された権限: root, root, 600	NFS 転送共有に指定された操作を実行した後、に予期される値とファイルの所有者、グループ、または権限が異なる理由を判別し、問題を修正します。
10.2	アプライアンスのクロックに対して、NFS サーバのクロックが同期されていません。時間差: 3 分 12 秒	NFS サーバとアプライアンスの時間設定を確認します。いずれか一方または両方が正確でない場合は、正しい時刻を設定し、NTP を使用して同期するようにします。
10.2	操作: chmod xyz の実行中に /opt/vmware/vcloud-director/data/transfer/xyz ファイルに予期しない権限が見つかりました。予期された権限: root root 750。検出された権限: root, root, 700	NFS 転送共有に指定された操作を実行した後、に予期される値とファイルの所有者、グループ、または権限が異なる理由を判別し、問題を修正します。
10.2	操作: chown xyz の実行中に /opt/vmware/vcloud-director/data/transfer/xyz ファイルに予期しない権限が見つかりました。予期された権限: root root 750。検出された権限: root, root, 700	NFS 転送共有に指定された操作を実行した後、に予期される値とファイルの所有者、グループ、または権限が異なる理由を判別し、問題を修正します。
10.2 以降	コマンドの引数が無効であるか、欠落しています。 usage: nfsValidate nfs_mount_string	JSON 要求の本文を解析できません。有効な JSON 要求の本文を指定します。
10.2 以降	nfs_mount 文字列が空です	NFS マウント文字列が要求の本文内にありません。NFS マウント文字列の引数を指定します。
10.2 以降	無効な nfs_mount 文字列: nfs_mount_string_argument	NFS マウント文字列を有効な形式 <i>IP_address:path</i> に変更します。
10.2 以降	無効なセル タイプ: cell_type_string	セル タイプは primary、standby、または cell である必要があります。OVF パラメータがこれらの値のいずれとも等しくない場合は、アプライアンスの構成を確認します。
10.2 以降	前提条件の OS 構成が完了しませんでした	/opt/vmware/appliance/etc/os-configuration-completed ファイルがアプライアンス内にありません。オペレーティング システムを構成します。
10.2 以降	Cloud Director アプライアンスのシステム セットアップはすでに完了しています。	/opt/vmware/appliance/etc/vcd-configuration-completed ファイルがアプライアンス上に見つかりました。クラウド ディレクトリのセットアップはすでに完了しているため、このスクリプトを実行しないでください。
10.2 以降	10.150.170.3:/data/transfer/cells ディレクトリはすでに存在します。プライマリ アプライアンスで、このディレクトリを削除する必要があります。	このディレクトリはプライマリ アプライアンスに配置しないでください。このディレクトリが NFS サーバ上に存在するため、削除する必要があります。

バージョン	エラー	アクション
10.2 以降	10.150.170.3:/data/transfer/appliance-nodes ディレクトリはすでに存在します。プライマリ アプライアンスで、このディレクトリを削除する必要があります。	このディレクトリはプライマリ アプライアンスに配置しないでください。このディレクトリが NFS サーバ上に存在するため、削除する必要があります。
10.2 以降	responses.properties ファイルは転送共有上にすでに存在します。プライマリ アプライアンスで、このディレクトリを削除する必要があります。	プライマリ アプライアンスに responses.properties ファイルを配置しないでください。削除する必要があります。
10.2 以降	responses.properties ファイルは転送共有上に存在しません。このファイルは、スタンバイ アプライアンスまたはセル アプライアンスにすでに存在している必要があります。	スタンバイ アプライアンスまたはセル アプライアンスに responses.properties ファイルが存在している必要があります。プライマリ アプライアンスがまだ構成されていない可能性があります。追加のセルを構成する前に、プライマリ アプライアンスを構成する必要があります。
10.2 以降	システム設定が進行中の場合は、nfsValidate を実行できません。	システムのセットアップが完了するまで待機してから、nfsValidate を実行します。
10.2 以降	このスクリプトで使用する一時ディレクトリを作成できません: /opt/vmware/vcloud-director/data/nfs-test	ファイル システムの権限を確認して、このディレクトリを作成できない理由を特定します。
10.2.1	指定された NFS 共有にファイルを作成できません。書き込み可能でない可能性があります。エクスポートされた NFS ファイルシステムが読み取り専用であるか、no_root_squash が指定されていないことが原因である可能性があります	マウントされた NFS 共有にアプライアンスが書き込みを実行できない理由を特定します。書き込みができない理由を確認するには、別の Linux マシンを使用して NFS 共有をマウントします。
10.2.1	指定された転送共有上のファイルに対して chmod を実行できません	マウントされた NFS 共有上のファイル システム オブジェクトのアクセス権限をこのアプライアンスが変更できない理由を特定します。別の Linux マシンを使用して NFS 共有をマウントします。
10.2.1	指定された転送共有上のファイルに対して chown を実行できません	マウントされた NFS 共有上のファイル システム オブジェクトの所有者をこのアプライアンスが変更できない理由を特定します。別の Linux マシンを使用して NFS 共有をマウントします。
10.2.1	マウント中にタイムアウトが発生しました	指定された NFS 共有をこのアプライアンスが 5 秒以内にマウントできない理由を特定します。NFS 共有を適切なタイミングでマウントできるかどうかを確認するには、別の Linux マシンを使用してマウントします。または、この NFS 共有の NFS サーバ エクスポート設定を確認します。

バージョン	エラー	アクション
10.2.1	マウント中にエラーが発生しました	このアプライアンスが指定された NFS 共有をマウントできない理由を特定します。NFS 共有をマウントできないかどうかを確認するには、別の Linux マシンを使用してマウントします。または、この NFS 共有の NFS サーバ エクスポート設定を確認します。
10.2.1	指定された NFS 共有は、UID 123 の不明なユーザーによって所有されています。root が予期されています 指定された NFS 共有は、GID 456 の不明なグループによって所有されています。root が予期されています	NFS 転送共有に指定された操作を実行した後、ファイルの所有者、グループ、またはその両方が予期される値と異なる理由を特定し、問題を修正します。
10.2.1	指定された NFS 共有に予期しない所有権または権限が見つかりました。予期された権限: root:root、モード 750。検出された権限: root:root、モード 777	NFS 転送共有に指定された操作を実行した後のファイルの所有者、グループ、およびモードに予期される値の一部またはすべてが想定どおりではない理由を特定します。問題を修正します。
10.2.1	アプライアンスのクロックに対して、NFS サーバのクロックが同期されていません。時間差: 1:55:14.603510	NFS サーバとアプライアンスの時間設定を確認します。いずれか一方または両方が正確でない場合は、正しい時刻を設定し、NTP を使用して同期するようにします。

VMware Cloud Director アプライアンスに移行またはリストアすると VMware Cloud Director サービスの再構成に失敗する

VMware Cloud 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

VMware Cloud Director を新しい VMware Cloud 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 VMware Cloud 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。

VMware Cloud Director アプライアンスのスタンバイ ノードがアクセス不能になる

VMware Cloud Director は、ノード間でストリーミング レプリケーションの同期を維持します。スタンバイ ノードがアクセス不能になった場合は、原因を特定して問題を解決する必要があります。

問題

VMware Cloud Director アプライアンス管理ユーザー インターフェイスにクラスタの健全性が DEGRADED と表示され、いずれかのスタンバイ ノードのステータスが unreachable になっています。

/nodes API は、localClusterHealth が DEGRADED に、ノードの status が unreachable に、nodeHealth が UNHEALTHY になっているという情報を返します。

たとえば、/nodes API がノードについて返す情報は以下ようになります。

```
{
  "localClusterFailover": "MANUAL",
  "localClusterHealth": "DEGRADED",
  "localClusterState": [
    {
      "connectionString": "host=primary_host_IP user=repmgr dbname=repmgr
connect_timeout=2",
      "failover": {
        "details": "failover = manual",
        "mode": "MANUAL",
        "repmgrd": {
          "details": "On node primary_node_ID (primary_host_name): repmgrd = not
applicable",
          "status": "NOT APPLICABLE"
        }
      },
      "id": primary_node_ID,
      "location": "default",
      "name": "primary_host_name",
      "nodeHealth": "HEALTHY",
      "nodeRole": "PRIMARY",
      "role": "primary",
      "status": "* running",
      "upstream": ""
    },
    {
      "connectionString": "host=unreachable_standby_host_IP user=repmgr dbname=repmgr
connect_timeout=2",
      "failover": {
        "details": "failover state unknown - unable to ssh to failed or unreachable
node",
        "mode": "UNKNOWN",
        "repmgrd": {
          "details": "On node unreachable_standby_node_ID
(unreachable_standby_host_name): repmgrd = n/a",
          "status": "UNKNOWN"
        }
      },
    },
  ],
}
```

```

        "id": unreachable_standby_node_ID,
        "location": "default",
        "name": "unreachable_standby_host_name",
        "nodeHealth": "UNHEALTHY",
        "nodeRole": "STANDBY",
        "role": "standby",
        "status": "? unreachable",
        "upstream": "primary_host_name"
    },
    {
        "connectionString": "host=running_standby_host_IP user=repmgr dbname=repmgr
connect_timeout=2",
        "failover": {
            "details": "failover = manual",
            "mode": "MANUAL",
            "repmgrd": {
                "details": "On node running_standby_node_ID (running_standby_host_IP):
repmgrd = not applicable",
                "status": "NOT APPLICABLE"
            }
        },
        "id": running_standby_node_ID,
        "location": "default",
        "name": "running_standby_host_name",
        "nodeHealth": "HEALTHY",
        "nodeRole": "STANDBY",
        "role": "standby",
        "status": "running",
        "upstream": "primary_host_name"
    }
],
"warnings": [
    "unable to connect to node \"unreachable_standby_host_name\" (ID:
unreachable_standby_node_ID)",
    "node \"unreachable_standby_host_name\" (ID: unreachable_standby_node_ID) is
registered as an active standby but is unreachable"
]
}

```

原因

データの整合性を維持するために、PostgreSQL データベースはログ先行書き込み (WAL) を使用します。プライマリ ノードは、レプリケーションおよびリカバリを行うために、WAL をアクティブなスタンバイ ノードに継続的にストリーミングします。WAL を受信したスタンバイ ノードは、WAL を処理します。スタンバイ ノードに到達できない場合、スタンバイ ノードは WAL の受信を停止し、新しいプライマリになるプロモーションの候補から外れます。

解決方法

- ◆ 到達不能なスタンバイ ノードの仮想マシンが実行されていることを確認します。
- ◆ スタンバイ ノードへのネットワーク接続が機能していることを確認します。
- ◆ スタンバイ ノードと他のノード間の通信を妨げる可能性がある SSH の問題がないことを確認します。

- ◆ スタンバイ ノードで vpostgres サービスが実行されていることを確認します。

次のステップ

ネットワークまたは SSH に問題がないことを確認するには、[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](#)を参照してください。

VMware Cloud Director アプライアンスのスタンバイ ノードが接続解除される

VMware Cloud Director は、ノード間でストリーミング レプリケーションの同期を維持します。スタンバイ ノードが接続解除された場合は、原因を特定して問題を解決する必要があります。

問題

VMware Cloud Director アプライアンス管理ユーザー インターフェイスにクラスタの健全性が DEGRADED と表示され、いずれかの接続解除されたスタンバイ ノードのステータスが running になり、感嘆符 (!) がスタンバイのアップストリーム ノードの名前の前に付いています。

PostgreSQL ログに、プライマリによって WAL セグメントが削除されたことが示されています。

```
2020-10-08 04:10:50.064 UTC [13390] LOG:  started streaming WAL from primary at 21/80000000
on timeline 17
2020-10-08 04:10:50.064 UTC [13390] FATAL:  could not receive data from WAL stream: ERROR:
requested WAL segment 0000001100000002100000080 has already been removed
2020-10-08 04:10:55.047 UTC [13432] LOG:  started streaming WAL from primary at 21/80000000
on timeline 17
2020-10-08 04:10:55.047 UTC [13432] FATAL:  could not receive data from WAL stream: ERROR:
requested WAL segment 0000001100000002100000080 has already been removed
```

/nodes API は、localClusterHealth が DEGRADED に、ノードの status が running に、nodeHealth が HEALTHY になっているという情報を返します。スタンバイのアップストリーム ノードの名前の前に感嘆符 (!)が付いていて、/nodes API から、スタンバイがアップストリーム ノードに接続されていないことを示す警告が返されません。

たとえば、/nodes API がノードについて返す情報は以下ようになります。

```
{
  "localClusterFailover": "MANUAL",
  "localClusterHealth": "DEGRADED",
  "localClusterState": [
    {
      "connectionString": "host=primary_host_IP user=repmgr dbname=repmgr
connect_timeout=2",
      "failover": {
        "details": "failover = manual",
        "mode": "MANUAL",
        "repmgrd": {
          "details": "On node primary_node_ID (primary_host_name): repmgrd = not
applicable",
          "status": "NOT APPLICABLE"
        }
      }
    },
  ],
}
```

```

        "id": primary_node_ID,
        "location": "default",
        "name": "primary_host_name",
        "nodeHealth": "HEALTHY",
        "nodeRole": "PRIMARY",
        "role": "primary",
        "status": "* running",
        "upstream": ""
    },
    {
        "connectionString": "host=unattached_standby_host_IP user=repmgr dbname=repmgr
connect_timeout=2",
        "failover": {
            "details": "failover = manual",
            "mode": "MANUAL",
            "repmgrd": {
                "details": "On node unattached_standby_node_ID
(unattached_standby_host_name): repmgrd = not applicable",
                "status": "NOT APPLICABLE"
            }
        },
        "id": unattached_standby_node_ID,
        "location": "default",
        "name": "unattached_standby_host_name",
        "nodeHealth": "HEALTHY",
        "nodeRole": "STANDBY",
        "role": "standby",
        "status": "running",
        "upstream": "! upstream_host_name"
    },
    {
        "connectionString": "host=running_standby_host_IP user=repmgr dbname=repmgr
connect_timeout=2",
        "failover": {
            "details": "failover = manual",
            "mode": "MANUAL",
            "repmgrd": {
                "details": "On node running_standby_node_ID (running_standby_host_name):
repmgrd = not applicable",
                "status": "NOT APPLICABLE"
            }
        },
        "id": running_standby_node_ID,
        "location": "default",
        "name": "running_standby_host_name",
        "nodeHealth": "HEALTHY",
        "nodeRole": "STANDBY",
        "role": "standby",
        "status": "running",
        "upstream": "upstream_host_name"
    }
],
"warnings": [

```

```
"node \"unattached_standby_host_name\" (ID: unattached_standby_node_ID) is not
attached to its upstream node \"upstream_host_name\" (ID: upstream_node_id) "
    ]
}
```

スタンバイ ノードが接続解除された場合は、できるだけ早く再接続する必要があります。ノードが接続解除されている期間が長すぎる場合、プライマリから WAL レコードを継続的にストリーミングする処理が遅れ、レプリケーションを再開できなくなることがあります。

原因

データの整合性を維持するために、PostgreSQL データベースはログ先行書き込み (WAL) を使用します。プライマリ ノードは、レプリケーションおよびリカバリを行うために、WAL をアクティブなスタンバイ ノードに継続的にストリーミングします。WAL を受信したスタンバイ ノードは、WAL を処理します。スタンバイ ノードが接続解除になると、スタンバイ ノードは WAL の受信を停止し、新しいプライマリになるプロモーションの候補から外れます。

解決方法

- 1 新しいスタンバイ ノードをデプロイします。
- 2 接続解除されたスタンバイ ノードを登録解除します。

次のステップ

[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](#)を参照してください。

クラスタの健全性で SSH の問題が示されている場合

データベース高可用性構成の VMware Cloud Director アプライアンス環境で、postgres ユーザーが SSH を介してピア データベース ノードに接続できません。

問題

データベース ノード間に SSH の問題がある場合は、VMware Cloud Director に `localClusterHealth` が `SSH_PROBLEM` として表示されます。この問題は重大であるため、可能なかぎり早く修正する必要があります。

`localClusterHealth` を表示するには、VMware Cloud Director アプライアンス管理ユーザー インターフェイスを使用するか、`/nodes` VMware Cloud Director アプライアンス API を実行します。[VMware Cloud Director アプライアンス API](#) のドキュメントを参照してください。

SSH 問題の発生したアプライアンス環境のピア ノードで `/nodes API` を実行すると、`/nodes API` は、`localClusterHealth` が `SSH_PROBLEM`、`localClusterFailover` が `INDETERMINATE` であるという情報を返します。`/nodes API` を実行しているノードから SSH 経由でピア ノードの 1 つに接続することができないため、フェイルオーバー モードは 不明 の状態です。SSH に問題のあるノードから送信されたレスポンス本文の "failover" 出力部分内の "details" に、`[ssh failed.command: ssh unreachable_standby_host_IP /usr/bin/grep failover=manual /opt/vmware/vpostgres/10/etc/repmgr.conf]` と表示されています。

たとえば、スタンバイ ノードに SSH 問題がある場合に、GET `https://primary_host_IP:5480/api/1.0.0/nodes` を実行すると、/nodes API は次の情報を返すことがあります。

```
{
  "localClusterFailover": "INDETERMINATE",
  "localClusterHealth": "SSH_PROBLEM",
  "localClusterState": [
    {
      "connectionString": "host=primary_host_IP user=repmgr dbname=repmgr
connect_timeout=2",
      "failover": {
        "details": "failover = manual",
        "mode": "MANUAL",
        "repmgrd": {
          "details": "On node primary_node_ID (primary_host_name): repmgrd = not
applicable",
          "status": "NOT APPLICABLE"
        }
      },
      "id": primary_node_ID,
      "location": "default",
      "name": "primary_host_name",
      "nodeHealth": "HEALTHY",
      "nodeRole": "PRIMARY",
      "role": "primary",
      "status": "* running",
      "upstream": ""
    },
    {
      "connectionString": "host=running_standby_host_IP user=repmgr dbname=repmgr
connect_timeout=2",
      "failover": {
        "details": "failover = manual",
        "mode": "MANUAL",
        "repmgrd": {
          "details": "On node running_standby_node_ID (running_standby_host_name):
repmgrd = not applicable",
          "status": "NOT APPLICABLE"
        }
      },
      "id": running_standby_node_ID,
      "location": "default",
      "name": "running_standby_host_name",
      "nodeHealth": "HEALTHY",
      "nodeRole": "STANDBY",
      "role": "standby",
      "status": "running",
      "upstream": "primary_host_name"
    },
    {
      "connectionString": "host=unreachable_standby_host_IP user=repmgr dbname=repmgr
connect_timeout=2",
      "failover": {
        "details": "ssh failed. command: ssh unreachable_standby_host_IP /usr/bin/
```

```

grep failover>manual /opt/vmware/vpostgres/10/etc/repmgr.conf",
    "mode": "UNKNOWN",
    "repmgrd": {
        "details": "On node unreachable_standby_node_ID
(unreachable_standby_host_name): repmgrd = not running",
        "status": "NOT RUNNING"
    }
},
"id": unreachable_standby_node_ID,
"location": "default",
"name": "unreachable_standby_host_name",
"nodeHealth": "HEALTHY",
"nodeRole": "STANDBY",
"role": "standby",
"status": "running",
"upstream": "primary_host_name"
}
],
"warnings": []
}

```

GET https://unreachable_standby_host_IP:5480/api/1.0.0/nodes を実行すると、ノードは信頼されていないため、localClusterFailover および localClusterState の情報が不正になることがあります。 / nodes API は、unreachable_standby_host_name がピア ノードに接続できないことを示す警告メッセージを返します。

たとえば、/nodes API が次の情報を返すことがあります。

```

{
    "localClusterFailover": "MANUAL",
    "localClusterHealth": "SSH_PROBLEM",
    "localClusterState": [
        {
            "connectionString": "host=primary_host_IP user=repmgr dbname=repmgr
connect_timeout=2",
            "failover": {
                "details": "ssh failed. command: ssh primary_host_IP /usr/bin/grep
failover>manual /opt/vmware/vpostgres/10/etc/repmgr.conf",
                "mode": "UNKNOWN",
                "repmgrd": {
                    "details": "On node primary_node_ID (primary_host_name): repmgrd = n/a",
                    "status": "UNKNOWN"
                }
            },
            "id": primary_node_ID,
            "location": "default",
            "name": "primary_host_name",
            "nodeHealth": "UNHEALTHY",
            "nodeRole": "PRIMARY",
            "role": "primary",
            "status": "? running",
            "upstream": ""
        },
        {

```

```

        "connectionString": "host=running_standby_host_IP user=repmgr dbname=repmgr
connect_timeout=2",
        "failover": {
            "details": "ssh failed. command: ssh running_standby_host_IP /usr/bin/grep
failover=manual /opt/vmware/vpostgres/10/etc/repmgr.conf",
            "mode": "UNKNOWN",
            "repmgrd": {
                "details": "On node running_standby_node_ID (running_standby_host_name):
repmgrd = n/a",
                "status": "UNKNOWN"
            }
        },
        "id": running_standby_node_ID,
        "location": "default",
        "name": "running_standby_host_name",
        "nodeHealth": "UNHEALTHY",
        "nodeRole": "STANDBY",
        "role": "standby",
        "status": "? running",
        "upstream": "primary_host_name"
    },
    {
        "connectionString": "host=unreachable_standby_host_IP user=repmgr dbname=repmgr
connect_timeout=2",
        "failover": {
            "details": "failover = manual",
            "mode": "MANUAL",
            "repmgrd": {
                "details": "On node unreachable_standby_node_ID
(unreachable_standby_host_name): repmgrd = not applicable",
                "status": "NOT APPLICABLE"
            }
        },
        "id": unreachable_standby_node_ID,
        "location": "default",
        "name": "unreachable_standby_host_name",
        "nodeHealth": "HEALTHY",
        "nodeRole": "STANDBY",
        "role": "standby",
        "status": "running",
        "upstream": "? primary_host_name"
    }
],
"warnings": [
    "unable to connect to node \"primary_host_name\" (ID: primary_node_ID)",
    "unable to connect to node \"running_standby_host_name\" (ID:
running_standby_node_ID)",
    "unable to connect to node \"unreachable_standby_host_name\" (ID:
unreachable_standby_node_ID)'s upstream node \"primary_host_name\" (ID: primary_node_ID)",
    "unable to determine if node \"unreachable_standby_host_name\" (ID:
unreachable_standby_node_ID) is attached to its upstream node \"primary_host_name\" (ID:
primary_node_ID)"
]
}

```

原因

VMware Cloud Director は、postgres の SSH 証明書を NFS 共有転送サーバ ストレージに保存します。すべてのデータベース ノードが共有転送サーバ ストレージにアクセスできる必要があります。データベース ノードが信頼されない状態になった場合、つまり、postgres ユーザーの SSH 証明書が有効でなくなったか、アクセス不能になった場合、そのノードは SSH クライアントを使用してピア ノードからコマンドを実行できません。HA モードの場合、VMware Cloud Director アプライアンスはこの機能を使用して適切に動作する必要があります。

解決方法

- 1 ノード間に接続の問題が発生しているかどうかを判断して、問題を修正します。[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](#)を参照してください。
- 2 次のコマンドを実行して、SSH 問題が発生したノードで `appliance-sync.timer` サービスが実行されていることを確認します。

```
systemctl status appliance-sync.timer
```

たとえば、コマンドによって以下が返される場合があります。

```
* appliance-sync.timer - Periodic check and sync of needed files for Cloud Appliance
functionality
   Loaded: loaded (/lib/systemd/system/appliance-sync.timer; enabled; vendor preset:
enabled)
   Active: active (waiting) since Sat 2020-09-05 23:22:49 UTC; 1 months 9 days ago

Warning: Journal has been rotated since unit was started. Log output is incomplete or
unavailable.
```

- 3 `appliance-sync.timer` サービスのステータスが **アクティブ** でない場合は、次のコマンドを実行してサービスを再起動します。

```
systemctl start appliance-sync.timer
```

- 4 約 90 秒間待機してから、VMware Cloud Director 管理ユーザー インターフェイスを使用するか `/nodes` API を呼び出して、クラスタの健全性が **健全** であることを確認します。

ログ ファイルを使用した VMware Cloud 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 VMware Cloud 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 VMware Cloud 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。

VMware Cloud Director のアップデートの確認に失敗する

VMware Cloud 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 VMware Cloud 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
```

VMware Cloud Director の最新アップデートのインストールに失敗する

VMware Cloud 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 VMware Cloud 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。

```
vam_cli update --install latest
```

Linux での VMware Cloud Director のインストール、アップグレード、お よび管理

4

1つ以上の Linux サーバに VMware Cloud Director ソフトウェアをインストールするか、VMware Cloud 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、VMware Cloud 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 VMware Cloud 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 VMware Cloud Director ソフトウェアには外部データベースが必要ですが、VMware Cloud 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。

VMware Cloud Director サーバ グループを作成したら、vSphere リソースに VMware Cloud 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、VMware Cloud 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 VMware Cloud Director インストールをアップグレードすると、VMware Cloud 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 VMware Cloud Director インストールを VMware Cloud Director アプライアンスに移行する場合は、VMware Cloud 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。

- 構成の計画
- VMware Cloud Director インストールの準備
- Linux への VMware Cloud Director のインストール
- VMware Cloud Director のインストール後
- Linux での VMware Cloud Director のアップグレード
- VMware Cloud Director のアップグレード後

構成の計画

vSphere は、VMware Cloud 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 VMware Cloud 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 VMware Cloud Director セルを割り当てます。
- すべてのターゲット VMware Cloud 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（VMware Cloud Director リリース ノートを参照）。
- Linux に VMware Cloud Director をインストールする場合は、[Linux での VMware Cloud Director の外部 PostgreSQL データベースの構成](#)の説明に沿って VMware Cloud Director データベースを設定します。

VMware Cloud Director インストールの準備

Linux サーバに VMware Cloud Director をインストールする前に、環境を準備する必要があります。

Linux での VMware Cloud Director の外部 PostgreSQL データベースの構成

VMware Cloud 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 VMware Cloud 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、VMware Cloud 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 VMware Cloud Director と一緒に使用する場合、特定の構成要件があります。

VMware Cloud 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。

VMware Cloud 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。

VMware Cloud 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 VMware Cloud 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 VMware Cloud Director のみです。VMware Cloud 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 VMware Cloud 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 VMware Cloud 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

VMware Cloud 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 VMware Cloud 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。

Linux での VMware Cloud Director の転送サーバ 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 ボリュームは VMware Cloud Director サーバー グループ内のすべてのサーバーからアクセスする必要があります。

サーバ グループの各メンバーは、このボリュームを同じマウントポイント (/opt/vmware/vcloud-director/data/transfer) にマウントします。このボリュームの領域は、次のような多くの方法で使用されます。

- 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てをお勧めします。
- 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 アイテムがこのボリュ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 ストレージのボリュームには、将来の拡張のための容量が必要です。

共有ストレージ オプション

従来の Linux ベースの NFS サーバやほかのソリューション（Microsoft Windows Server、VMware vSAN File Service の NFS 機能など）では、共有ストレージを使用できます。vSAN 7.0 以降では、vSAN File Service 機能で NFS 3.0 および NFS 4.1 プロトコルを使用して、NFS 共有をエクスポートすることができます。vSAN File Service の詳細については、[VMware vSphere 製品のドキュメント](#)の『Administering VMware vSAN』ガイドを参照してください。

NFS サーバを構成するための要件

NFS サーバの構成には、VMware Cloud 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、VMware Cloud 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、VMware Cloud 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。

Linux NFS サーバの例

Linux NFS サーバに、VMware Cloud 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、vCD-Cell2-IP、vCD-Cell3-IP という名前の 3 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メソッドは、`no_root_squash` メソッドです。`/etc/exports` ファイルに次の行を追加する必要があります。

```
/nfs/vCDspace vCD_Cell1_IP_Address(rw,sync,no_subtree_check,no_root_squash)
/nfs/vCDspace vCD_Cell2_IP_Address(rw,sync,no_subtree_check,no_root_squash)
/nfs/vCDspace vCD_Cell3_IP_Address(rw,sync,no_subtree_check,no_root_squash)
```

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。

VMware Cloud Director サーバ グループ内のサーバのすべてがこの NFS 共有をマウントできるように、NFS サーバの `/etc/exports` ファイルに、これらのサーバに対応するエントリが必要になります。NFS サーバ上の `/etc/exports` ファイルに変更を加えた後、`exportfs -a` を実行して、すべての NFS 共有を再度エクスポートします。

VMware Cloud 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

VMware Cloud 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 VMware Cloud 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。

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、VMware Cloud 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。VMware Cloud 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。

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

VMware Cloud 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 VMware Cloud 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。VMware Cloud 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 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、[VMware Cloud 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、VMware Cloud 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。VMware Cloud 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、[Linux での VMware Cloud 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、VMware Cloud Director インストールで VMware Cloud 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。

VMware Cloud 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 クラスター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。

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

VMware Cloud 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。

VMware Cloud 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、[VMware Cloud 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、VMware Cloud 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。VMware Cloud 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、[Linux での VMware Cloud 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 ゾーンを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

VMware Cloud 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、『VMware Cloud 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、『VMware Cloud 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、『VMware Cloud Director Service Provider Admin Portal Guide』を参照してください。

Linux への VMware Cloud Director のインストール

1 つ以上の Linux サーバの VMware Cloud Director ソフトウェアをインストールすることで、VMware Cloud 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 VMware Cloud Director インストールをアップグレードする場合は、[Linux での VMware Cloud Director のアップグレード](#)を参照してください。

重要： Linux 上の VMware Cloud Director インストールおよび VMware Cloud 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。

バージョン 10.1 以降では、サービス プロバイダとテナントは VMware Cloud Director API を使用してリモート サーバへの接続をテストし、サーバ ID を SSL ハンドシェイクの一部として検証できます。VMware Cloud Director ネットワーク接続を保護するために、VMware Cloud Director API を使用して接続テストを行っているテナントからは到達できない内部ホストの拒否リストを構成します。VMware Cloud Director のインストールまたはアップグレードの後、テナントに VMware Cloud Director へのアクセスを許可する前に、拒否リストを構成します。[テスト接続拒否リストの構成](#)を参照してください。

前提条件

- サーバ グループのターゲット サーバが [2 章 VMware Cloud 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 VMware Cloud Director に SSL 証明書を作成する前に](#)を参照してください。
- VMware Cloud 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。[Linux での VMware Cloud Director の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 VMware Cloud Director データベースを作成したことを確認します。『[Linux での VMware Cloud 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 VMware Cloud 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、[VMware Cloud 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 VMware Cloud Director サーバとデータベース サーバが、[VMware Cloud 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 VMware Cloud 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。VMware Cloud 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 VMware Cloud 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 VMware Cloud Director インストーラを実行して VMware Cloud Director サーバ グループの作成を開始することができます。

2 Linux 上の VMware Cloud Director 向けの SSL 証明書の作成と管理

VMware Cloud 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 VMware Cloud 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。

3 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 VMware Cloud 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。

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

VMware Cloud 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。『[VMware Cloud 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 VMware Cloud 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 VMware Cloud Director インストーラを実行して VMware Cloud Director サーバ グループの作成を開始することができます。

VMware Cloud 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-nnnnnnn.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、VMware Cloud Director がインストールまたはアップグレードされます。

VMware Cloud 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、VMware Cloud 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@cell11 /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、VMware Cloud Director インストール ファイルへのフル パス名です。

```
[root@cell11 /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@cell11 /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 VMware Cloud 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。

Linux 上の VMware Cloud Director 向けの SSL 証明書の作成と管理

VMware Cloud 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 VMware Cloud 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。

Linux 上の VMware Cloud Director に SSL 証明書を作成する前に

VMware Cloud 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 VMware Cloud Director をインストールしてから作成する必要があります。VMware Cloud 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 VMware Cloud 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 VMware Cloud 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 VMware Cloud 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 VMware Cloud 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 VMware Cloud 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 VMware Cloud Director の SSL を構成するのに便利な方法です。

各 VMware Cloud 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 VMware Cloud 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 VMware Cloud 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。VMware Cloud 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 VMware Cloud 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 VMware Cloud 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 VMware Cloud 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 VMware Cloud 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 VMware Cloud 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 VMware Cloud 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。VMware Cloud 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 VMware Cloud 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、[HTTPS 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、[HTTPS 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 VMware Cloud 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。VMware Cloud 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 PKCS12 -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 PKCS12 -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 PKCS12 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 PKCS12 -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 PKCS12 -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 PKCS12 -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 PKCS12 -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 PKCS12 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 PKCS12 -storepass keystore_password -keystore certificates.ks -list
```

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

次のステップ

- VMware Cloud 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 VMware Cloud 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。

- VMware Cloud 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。 [HTTPS 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 VMware Cloud 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 VMware Cloud 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 VMware Cloud 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。VMware Cloud 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 VMware Cloud 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、[HTTPS 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.p12 -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.p12 -chain
```

3 keytool を使用して、PKCS12 キーストアを certificate.ks 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 PKCS12 -srckeystore http.pl2 -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 PKCS12 -srckeystore consoleproxy.pl2 -srcstoretype PKCS12 -srcstorepass
keystore_password
```

4 証明書が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 PKCS12 -storepass keystore_password -keystore certificates.ks -list
```

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

次のステップ

- VMware Cloud 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 VMware Cloud 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。

- VMware Cloud 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。 [HTTPS 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。

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 VMware Cloud 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。

VMware Cloud 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。VMware Cloud 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。

HTTPS 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、「[5 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 VMware Cloud 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 VMware Cloud 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。

- a 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。
- b VMware Cloud Director サービスが開始した後に [VMware Cloud 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。
- c VMware Cloud Director セルを起動するよう指示します。

3 (オプション) [VMware Cloud 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 VMware Cloud 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 4-1. 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
HTTPS 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。 注： HTTPS 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	Linux 上の VMware Cloud Director に SSL 証明書を作成する前に参照してください。
HTTPS SSL 証明書のプライベート キーのパスワード	Linux 上の VMware Cloud Director に SSL 証明書を作成する前に参照してください。
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	Linux 上の VMware Cloud Director に SSL 証明書を作成する前に参照してください。
Syslog ホストへのリモート監査ログ記録の有効化	各 VMware Cloud Director セル内のサービスは、監査メッセージを VMware Cloud 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 VMware Cloud Director データベースだけでなく <code>syslog</code> ユーティリティに送信するように VMware Cloud Director サービスを構成します。 ■ スキップする場合は、Enter キーを押します。 ■ 有効にする場合は、Syslog ホストの名前または IP アドレスを入力します。
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 <code>vcloud</code> です。

表 4-1. 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
データベース ユーザー名	『Linux での VMware Cloud Director の外部 PostgreSQL データベースの構成』を参照してください。
データベースのパスワード	『Linux での VMware Cloud Director の外部 PostgreSQL データベースの構成』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 & 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。5 章 セル管理ツール リファレンスを参照してください。</p> <p>プログラムに参加する場合は、y 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、n 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 4-2. 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
<code>--help(-h)</code>	なし	構成オプションと引数値のサマリを表示します。
<code>--config-file (-c)</code>	<code>global.properties</code> 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 <code>/opt/vmware/vcloud-director/etc/global.properties</code> になります。
<code>--console-proxy-ip (-cons)</code>	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 VMware Cloud 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、 <code>10.17.118.159</code> とします。
<code>--console-proxy-port-https</code>	0~65535 の整数	VMware Cloud Director コンソール プロキシ サービスが使用するポート番号。

表 4-2. 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
--database-ssl	true または false	適切に署名された SSL 接続が VMware Cloud 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、「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。
--database-host(-dbhost)	VMware Cloud 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	『Linux での VMware Cloud Director の外部 PostgreSQL データベースの構成』を参照してください。
--database-name(-dbname)	データベース サービス名	『Linux での VMware Cloud Director の外部 PostgreSQL データベースの構成』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。	『Linux での VMware Cloud Director の外部 PostgreSQL データベースの構成』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	『Linux での VMware Cloud Director の外部 PostgreSQL データベースの構成』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。 『Linux での VMware Cloud Director の外部 PostgreSQL データベースの構成』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	『Linux での VMware Cloud Director の外部 PostgreSQL データベースの構成』を参照してください。
--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 (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。5 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

表 4-2. 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
--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 VMware Cloud Director Web インターフェイス サービスに使用します。たとえば、 <i>10.17.118.159</i> とします。
--primary-port-http	0～65535 の整数	VMware Cloud 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	VMware Cloud 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 VMware Cloud Director セル内のサービスは、監査メッセージを VMware Cloud 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 VMware Cloud 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 VMware Cloud 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。
--response-file (-r)	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、/opt/vmware/vcloud-director/etc/responses.properties 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。 重要： 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。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。
--unattended-installation (-unattended)	なし	無人でのインストールを指定します。
--keystore-password (-w)	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、HTTPS 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 VMware Cloud Director サーバの無人構成を実行します。

```
[root@cell11 /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 P@55word -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、HTTPS 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 VMware Cloud Director サーバの無人構成を実行します。

```
[root@cell11 /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 P@55word -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 VMware Cloud 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する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は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 VMware Cloud 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@cell11 /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@cell11 /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 VMware Cloud Director のインストール

VMware Cloud 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 VMware Cloud Director インストールおよび VMware Cloud 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 VMware Cloud 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、VMware Cloud Director インストール ファイルへのフル パス名です。

```
[root@cell11 /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@cell11 /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 VMware Cloud 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 VMware Cloud 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 このサーバー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、VMware Cloud 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 VMware Cloud 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。

VMware Cloud Director サービスがすべてのサーバ上で稼動しているときに、VMware Cloud 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。『[VMware Cloud Director インストール環境の構成](#)』を参照してください。

VMware Cloud Director のインストール後

VMware Cloud 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 を構成し、データベース上の一部のパラメータを調整できます。

バージョン 10.1 以降では、サービス プロバイダとテナントは VMware Cloud Director API を使用してリモートサーバへの接続をテストし、サーバ ID を SSL ハンドシェイクの一部として検証できます。VMware Cloud Director ネットワーク接続を保護するために、VMware Cloud Director API を使用して接続テストを行っているテナントからは到達できない内部ホストの拒否リストを構成します。VMware Cloud Director のインストールまたはアップグレードの後、テナントに VMware Cloud Director へのアクセスを許可する前に、拒否リストを構成します。[テスト接続拒否リストの構成](#)を参照してください。

Linux での VMware Cloud Director 用パブリック 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、VMware Cloud Director Web ポータル、VMware Cloud Director 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。

前提条件

システム管理者としてログインしていることを確認します。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 Service Provider Admin Portal の上部ナビゲーション バーで [管理] を選択します。
- 2 左側のペインの [設定] で、[公開アドレス] をクリックします。
- 3 公開エンドポイントをカスタマイズするには、[編集] をクリックします。
- 4 VMware Cloud 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 VMware Cloud 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 VMware Cloud 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す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 VMware Cloud 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）Cloud Director 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 VMware Cloud Director API に、`http://vcloud.example.com/cloudapi` から VMware Cloud Director 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 VMware Cloud Director API に、`https://vcloud.example.com/cloudapi` から VMware Cloud Director 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す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 VMware Cloud 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 VMware Cloud 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、VMware Cloud 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: VMware Cloud 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、VMware Cloud 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。

VMware Cloud 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

VMware Cloud 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。VMware Cloud 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 VMware Cloud 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、VMware Cloud 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、『VMware Cloud 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、VMware Cloud 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@cell11 /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、「[5 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) VMware Cloud 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@cell11 /opt/vmware/vcloud-director/
bin]# ./cell-management-tool cassandra --add-rollup \ --username admin --password
'P@55w0rd'
```

- 3 各 VMware Cloud 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

VMware Cloud 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 VMware Cloud 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 VMware Cloud 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 VMware Cloud 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 VMware Cloud Director セルから VMware Cloud 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@cell11 /opt/vmware/vcloud-director/
bin]#cell-management-tool import-trusted-certificates --source path_to_self-
signed_or_private_cert
```

- b VMware Cloud 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@cell11 /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@cell11 /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、[5 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 VMware Cloud 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。

RabbitMQ AMQP ブローカのインストールおよび構成

ブロック タスク、通知、VMware Cloud Director API 拡張機能（Container Service Extension (CSE) や VMware Cloud Director App Launchpad など）を使用するには、RabbitMQ AMQP ブローカをインストールし構成する必要があります。

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。VMware Cloud 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。

VMware Cloud Director では、通知を構成する際に、RabbitMQ AMQP ブローカの代わりに MQTT クライアントを使用できます。 [MQTT クライアントを使用したイベント、タスク、およびメトリックへのサブスクライブ](#)を参照してください。

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、『VMware Cloud 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 VMware Cloud 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 VMware Cloud Director を構成するときに必要な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。非 SSL では、デフォルトは 5672 です。SSL/TLS のデフォルト ポートは 5671 です。
- 通信プロトコルは TCP 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、VMware Cloud 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。VMware Cloud 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 `$VCLOUD_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。

VMware Cloud Director AMQP サービスで SSL を有効にするには、『VMware Cloud Director Service Provider Admin Portal Guide』の [AMQP ブローカの構成](#)の情報を参照してください。

MQTT クライアントを使用したイベント、タスク、およびメトリックへのサブスクリプション

MQTT クライアントを使用して、VMware Cloud Director のイベントおよびタスクに関するメッセージをサブスクリプションすることができます。

MQTT は、軽量でバイナリ形式のメッセージ転送プロトコルです。VMware Cloud Director は MQTT を使用して、MQTT クライアントを使用してサブスクリプションできるイベントおよびタスクに関する情報を公開します。

MQTT メッセージは MQTT ブローカを通過しますが、クライアントがオンラインでないとき、MQTT ブローカはメッセージを保存することもできます。

VMware Cloud Director 10.2.2 以降では、MQTT クライアントを使用してメトリックにサブスクリプションできます。

前提条件

- WebSocket をサポートする MQTT クライアントがあることを確認します。
- WebSocket にアップグレードされた要求にヘッダーを追加できることを確認します。
- メトリックにサブスクリプションする場合は、メトリックの収集を構成し、メトリックの公開を有効にします。 [メトリックの収集と公開の構成](#)を参照してください。

手順

- 1 OpenAPI エンドポイントを使用して VMware Cloud Director にログインします。
- 2 WebSocket 接続を確立するには、Sec-WebSocket-Protocol プロパティを `mqtt` に設定し、クライアントが `/messaging/mqtt` パスに接続するように設定し、認証ヘッダーを追加して、標準の MQTT 接続フローを実行します。

VMware Cloud Director に対する標準のログイン要求から JWT トークンを受け取ります。ユーザー名とパスワードは空のままにすることができます。

```
Sec-WebSocket-Protocol: mqtt
```

```
Authorization: Bearer {JWT_token}
```

- 3 接続が正常に確立されたら、MQTT クライアントを通じてトピックをサブスクリプションします。

```
publish/{user_org_id}/{user_id}
```

```
publish/debd63a0-6eae-11ea-8c7b-0050561776be/d19fd8ff-6eae-11ea-bb42-0050561776c8
```

組織管理者は、ワイルドカードを使用してすべての組織のトピックにアクセスできます。

```
publish/{user_org_id}/+
```

システム管理者は、ワイルドカードを使用してすべてのトピックにアクセスできます。

```
publish/#
```

4 (オプション) VMware Cloud Director 10.2.2 以降では、メトリックにサブスクライブします。

```
metrics/{org_id}/{vApp_id}
```

メトリックのトピックにアクセスできるのは、システム管理者のみです。

自動スケール グループ

VMware Cloud Director 10.2.2 以降では、テナント ユーザーに、現在の CPU およびメモリの使用量に応じて、アプリケーションを自動スケールする許可を与えることができます。

CPU およびメモリの使用量について事前定義された基準に応じて、テナントは VMware Cloud Director を使用して、選択したスケール グループ内の仮想マシンの数を自動的に増減できます。テナントがアプリケーションを自動スケールできるようにするには、自動スケール ソリューションへのアクセス権を構成、公開、および付与する必要があります。

同じアプリケーションを実行するように構成したサーバの負荷を分散させるには、VMware NSX Advanced Load Balancer (Avi Networks) を使用します。

自動スケール プラグインの構成と公開

テナントへのアクセス権を付与する前に、自動スケール グループ ソリューションを構成する必要があります。自動スケールは VMware Cloud Director 10.2.2 以降で使用できます。

- 1 クラスタ内のいずれかのセルの OS に root として直接、または SSH クライアントを使用してログインします。
- 2 Cassandra データベースでメトリック収集を設定して、メトリック データの収集を有効にするか、メトリック データの永続性なしでメトリックを収集します。

- [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](#)
- データの永続性なしでメトリック データを収集するには、次のコマンドを実行します。

```
/opt/vmware/vcloud-director/bin/cell-management-tool manage-config -n
statsFeeder.metrics.collect.only -v true
```

- 3 メトリックの公開を有効にします。

```
/opt/vmware/vcloud-director/bin/cell-management-tool manage-config -n
statsFeeder.metrics.publishing.enabled -v true
```

- 4 /tmp フォルダ内に、次の内容を含む metrics.groovy ファイルを作成します。

```
configuration {
    metric("cpu.ready.summation") {
        currentInterval=20
        historicInterval=20
        entity="VM"
        instance=""
    }
}
```

```

        minReportingInterval=300
        aggregator="AVERAGE"
    }
}

```

- 5 ファイルをインポートします。

```

$VCLLOUD_HOME/bin/cell-management-tool configure-metrics --metrics-config /tmp/
metrics.groovy

```

- 6 以前に Cassandra を構成している場合は、適切なノード アドレス、データベース認証の詳細、ポートおよびメトリックの有効日数を指定して Cassandra スキーマを更新します。

```

$VCLLOUD_HOME/bin/cell-management-tool cassandra -configure -cluster-nodes
nodes_IP_addresses -username cassandra -password cassandra_password -port port_number -ttl
TTL_days -update-schema

```

- 7 CA 署名付き証明書を使用してセルを実行する場合、自動スケール有効にするには、次のコマンドを実行します。

```

$VCLLOUD_HOME/bin/cell-management-tool configure-autoscale --set enabled=true
$VCLLOUD_HOME/bin/cell-management-tool configure-autoscale --set username=<username>
$VCLLOUD_HOME/bin/cell-management-tool configure-autoscale --encrypt --set
password=<password>

```

ターミナルからコマンドを実行する場合は、バックスラッシュ (\) 記号を使用して特殊文字をエスケープします。

- 8 セルを再起動します。

```

service vmware-vcd restart

```

9 自動スケール権限バンドルの公開

自動スケール権限バンドルの公開

テナントがアプリケーションを自動スケールする場合は、システム内の 1 つ以上の組織に権限バンドルを公開する必要があります。自動スケールは VMware Cloud Director 10.2.2 以降で使用できます。

前提条件

自動スケール プラグインの構成と公開

手順

- 1 上部ナビゲーション バーで [管理] を選択します。
- 2 左側のパネルの [テナント アクセス コントロール] で、[権限バンドル] を選択します。
- 3 自動スケールへのアクセス権を付与するテナント組織に、レガシー権限バンドルがないことを確認します。
- 4 vmware:scalegroup Entitlement バンドルを選択して、[公開] をクリックします。

5 バンドルを公開するには：

- a [テナントに公開] を選択します。
- b ロールを公開する組織を選択します。
 - バンドルをシステム内のすべての既存の組織および新規に作成された組織に公開する場合は、[すべてのテナントに公開] を選択します。
 - システム内の特定の組織にバンドルを公開する場合は、組織を個別に選択します。

6 [保存] をクリックします。

次のステップ

自動スケールを使用するテナント ロールに必要な VMWARE:SCALEGROUP 権限を追加します。「VMware Cloud Director Service Provider Admin Portal Guide」の[グローバル テナント ロールの表示と編集](#)を参照してください。

Linux での VMware Cloud Director のアップグレード

VMware Cloud 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 VMware Cloud 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、VMware Cloud Director データベースをアップグレードしてから、VMware Cloud Director セルを再起動します。

既存の VMware Cloud Director サーバ グループが Linux の VMware Cloud Director インストール環境から構成される場合は、Linux 用の VMware Cloud 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。

Linux に VMware Cloud 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 VMware Cloud Director をアップグレードすることができます。[VMware Cloud 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[VMware Cloud 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。

VMware Cloud 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 VMware Cloud 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、[アップグレードのパスとワークフロー](#)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、すべての ESXi 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。
- VMware Cloud 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。

VMware Cloud 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。

VMware Cloud 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。

- VMware Cloud 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。
- VMware Cloud Director と直接通信するサードパーティ製コンポーネント。

VMware Cloud 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 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。VMware Cloud 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、VMware Cloud 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。[VMware Cloud Director のアップグレード後](#)を参照してください。

1 台以上の VMware Cloud Director サーバをアップグレードしてから、VMware Cloud 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 VMware Cloud 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、VMware Cloud 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せん。

- 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 VMware Cloud 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。

バージョン 10.1 以降では、サービス プロバイダとテナントは VMware Cloud Director API を使用してリモート サーバへの接続をテストし、サーバ ID を SSL ハンドシェイクの一部として検証できます。VMware Cloud Director ネットワーク接続を保護するために、VMware Cloud Director API を使用して接続テストを行っているテナントからは到達できない内部ホストの拒否リストを構成します。VMware Cloud Director のインストールまたはアップグレードの後、テナントに VMware Cloud Director へのアクセスを許可する前に、拒否リストを構成します。[テスト接続拒否リストの構成](#)を参照してください。

重要： バージョン 10.1 以降にアップグレードすると、VMware Cloud Director は常に、自身に接続されているすべてのインフラストラクチャ エンドポイントの証明書を検証します。これは、VMware Cloud Director での SSL 証明書の管理方法が変更されたためです。アップグレード前に証明書を VMware Cloud Director にインポートしていない場合は、vCenter Server と NSX の接続が、SSL 検証の問題が原因の接続エラーで失敗したと表示されることがあります。この場合、アップグレード後に、次の 2 つの方法のいずれかを実行できます。

- 1 セル管理ツールで `trust-infra-certs` コマンドを実行して、すべての証明書を中央の証明書ストアに自動的にインポートします。[vSphere リソースからのエンドポイント証明書のインポート](#)を参照してください。
- 2 Service Provider Admin Portal ユーザー インターフェイスで、各 vCenter Server および NSX インスタンスを選択し、証明書を承認する際に資格情報を再入力します。

アップグレードのパスとワークフロー

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 VMware Cloud Director 10.2
外部 Microsoft SQL Server データベースを使用する Linux 上の VMware Cloud Director 9.7	<ol style="list-style-type: none"> 1 Microsoft SQL Server データベースを PostgreSQL データベースに移行します。PostgreSQL データベースへの移行を参照してください。 2 環境を Linux 上の VMware Cloud Director 10.2 にアップグレードします。VMware Cloud 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VMware Cloud 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。
外部 PostgreSQL データベースを使用する Linux 上の VMware Cloud Director 9.7、10.0、または 10.1	環境を Linux 上の VMware Cloud Director 10.2 にアップグレードします。 VMware Cloud 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 VMware Cloud 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。
組み込みの PostgreSQL データベースを使用する VMware Cloud Director アプライアンス 9.7、10.0、および 10.1	サポート対象外

VMware Cloud 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 VMware Cloud 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 VMware Cloud Director インストーラを使用すると、サポート対象 Linux OS 上の VMware Cloud Director インストール環境で構成される VMware Cloud Director サーバ グループをアップグレードできます。VMware Cloud Director サーバ グループが VMware Cloud Director 9.5 アプライアンス環境で構成される場合、Linux 用の VMware Cloud 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。[VMware Cloud Director アプライアンスのアップグレードと移行](#)を参照してください。

VMware Cloud 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-nnnnnnn.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、VMware Cloud 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 VMware Cloud 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

- VMware Cloud 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 VMware Cloud Director と互換性があることを確認します。

重要： 既存の VMware Cloud 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、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、[Linux での VMware Cloud 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 VMware Cloud 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： VMware Cloud Director プロセスを実行する ID として使用するため、VMware Cloud 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。無効になっている 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。[Linux での VMware Cloud Director の転送サーバ ストレージの準備](#)を参照してください。
- VMware Cloud 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@cell11 /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、VMware Cloud Director インストール ファイルへのフル パス名です。

```
[root@cell11 /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 VMware Cloud 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、VMware Cloud 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 VMware Cloud Director RPM パッケージを展開する。
- 3 現在のセルで VMware Cloud Director ソフトウェアをアップグレードします。
- 4 VMware Cloud 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 VMware Cloud Director ソフトウェアをアップグレードしてから、各セルで VMware Cloud Director サービスを再起動します。
- 6 現在のセルで VMware Cloud 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 VMware Cloud 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。

VMware Cloud 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 VMware Cloud 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 VMware Cloud Director インストーラを使用すると、サポート対象 Linux OS 上の VMware Cloud Director インストール環境で構成される VMware Cloud Director サーバ グループをアップグレードできます。VMware Cloud Director サーバ グループが VMware Cloud Director 9.5 アプライアンス環境で構成される場合、Linux 用の VMware Cloud 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。[VMware Cloud Director アプライアンスのアップグレードと移行](#)を参照してください。

複数セルの VMware Cloud 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、VMware Cloud 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。[VMware Cloud 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

- VMware Cloud 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 VMware Cloud Director と互換性があることを確認します。

重要： 既存の VMware Cloud 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、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、[Linux での VMware Cloud Director のアップグレード](#)を参照してください。

- VMware Cloud 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 VMware Cloud 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。無効になっている ESXi ホストはサポートされません。

手順

1 VMware Cloud Director セルのアップグレード

VMware Cloud 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 VMware Cloud Director ソフトウェアをアップグレードします。

2 VMware Cloud Director データベースのアップグレード

アップグレードした VMware Cloud Director サーバで、VMware Cloud 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 VMware Cloud 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 VMware Cloud 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 VMware Cloud 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。

VMware Cloud Director セルのアップグレード

VMware Cloud 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 VMware Cloud Director ソフトウェアをアップグレードします。

VMware Cloud 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-nnnnnnn.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、VMware Cloud 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 VMware Cloud Director インストールの場合は、VMware Cloud Director サーバ グループのメンバーごとに VMware Cloud 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@cell11 /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、VMware Cloud Director インストール ファイルへのフル パス名です。

```
[root@cell11 /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@cell11 /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、VMware Cloud 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 VMware Cloud 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 VMware Cloud Director RPM パッケージを展開する。
- c セル上のすべてのアクティブ VMware Cloud Director ジョブが完了すると、サーバ上で VMware Cloud Director サービスが停止し、インストール済みの VMware Cloud 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 /opt/vmware/vcloud-director/etc/log4j.properties 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、/opt/vmware/vcloud-director/etc/log4j.properties.rpmnew を既存の /opt/vmware/vcloud-director/etc/log4j.properties ファイルにマージします。

結果

VMware Cloud 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、VMware Cloud 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 VMware Cloud 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、VMware Cloud Director サービスを起動しないでください。

VMware Cloud Director データベースのアップグレード

アップグレードした VMware Cloud Director サーバで、VMware Cloud 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 VMware Cloud 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、VMware Cloud 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。

VMware Cloud 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 VMware Cloud 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 VMware Cloud 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 VMware Cloud 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、『[5 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、稼動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 VMware Cloud 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 VMware Cloud 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 VMware Cloud 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。[VMware Cloud 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 4-3. 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
--backup-completed	なし	VMware Cloud 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。
--ceip-user	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: phone-home-system-account。

表 4-3. 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
--enable-ceip	次のいずれかを選択します <ul style="list-style-type: none"> ■ true ■ false 	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 false に設定されていないとき、デフォルトは true 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、 http://www.vmware.com/trustvmware/ceip.html 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。『5 章 セル管理ツール リファレンス』を参照してください。
--installer-path	VMware Cloud 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、VMware Cloud 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。

表 4-3. 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
--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、 VMware Cloud 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。
--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： VMware Cloud Director プロセスを実行する ID として使用するため、VMware Cloud 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。

VMware Cloud Director のアップグレード後

すべての VMware Cloud Director サーバと共有データベースをアップグレードした後、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、VMware Cloud 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： VMware Cloud Director では、詳細 Edge Gateway のみがサポートされます。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。

バージョン 10.1 以降では、サービス プロバイダとテナントは VMware Cloud Director API を使用してリモート サーバへの接続をテストし、サーバ ID を SSL ハンドシェイクの一部として検証できます。VMware Cloud Director ネットワーク接続を保護するために、VMware Cloud Director API を使用して接続テストを行っているテナントからは到達できない内部ホストの拒否リストを構成します。VMware Cloud Director のインストールまたはアップグレードの後、テナントに VMware Cloud Director へのアクセスを許可する前に、拒否リストを構成します。[テスト接続拒否リストの構成](#)を参照してください。

重要： バージョン 10.1 以降にアップグレードすると、VMware Cloud Director は常に、自身に接続されているすべてのインフラストラクチャ エンドポイントの証明書を検証します。これは、VMware Cloud Director での SSL 証明書の管理方法が変更されたためです。アップグレード前に証明書を VMware Cloud Director にインポートしていない場合は、vCenter Server と NSX の接続が、SSL 検証の問題が原因の接続エラーで失敗したと表示されることがあります。この場合、アップグレード後に、次の 2 つの方法のいずれかを実行できます。

- 1 セル管理ツールで `trust-infra-certs` コマンドを実行して、すべての証明書を中央の証明書ストアに自動的にインポートします。[vSphere リソースからのエンドポイント証明書のインポート](#)を参照してください。
- 2 Service Provider Admin Portal ユーザー インターフェイスで、各 vCenter Server および NSX インスタンスを選択し、証明書を承認する際に資格情報を再入力します。

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

VMware Cloud 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、VMware Cloud Director セルが実行中であるかどうかにかかわらず、VMware Cloud 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 VMware Cloud 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

VMware Cloud Director および NSX Manager のアップグレードが終わったら、VMware Cloud 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。
 - a VMware Cloud Director Service Provider Admin Portal の上部ナビゲーション バーで、[リソース] の下にある [vSphere リソース] を選択します。
 - b 左側のパネルで [vCenter Server インスタンス] をクリックします。
 - c 無効にする vCenter Server インスタンスの横にあるラジオ ボタンを選択して、[無効化] をクリックします。
 - d [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 VMware Cloud Director パブリック URL および証明書チェーンを確認します。
 - a 上部ナビゲーション バーで [管理] を選択します。
 - b 左側のパネルの [設定] で、[公開アドレス] をクリックします。
 - c 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 VMware Cloud Director で更新します。
 - a VMware Cloud Director Service Provider Admin Portal の上部ナビゲーション バーで、[リソース] の下にある [vSphere リソース] を選択します。
 - b 左側のパネルで [vCenter Server インスタンス] をクリックします。
 - c 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。
 - d [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 VMware Cloud 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/jp/>) を参照してください。
- VMware Cloud 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 VMware Cloud 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。
- VMware Cloud Director または VMware Cloud Director 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、『VMware Cloud Director 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、VMware Cloud 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。

セル管理ツール リファレンス

5

セル管理ツールは、VMware Cloud 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@cell11 /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
```

■ VMware Cloud 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。

■ 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

VMware Cloud 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 VMware Cloud Director へのアクセスに、個別の VMware Cloud 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、VMware Cloud 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

VMware Cloud 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。

■ HTTPS 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、HTTPS 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。

■ HTTPS 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、HTTPS 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 VMware Cloud 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。

■ vSphere リソースからのエンドポイント証明書のインポート

アップグレード後、セル管理ツールの `trust-infra-certs` コマンドを使用して、環境内の vSphere リソースから VMware Cloud Director データベースに証明書を収集してインポートします。

■ テスト接続拒否リストの構成

インストールまたはアップグレード後、VMware Cloud Director ネットワークへのアクセスをテナントに許可する前に、セル管理ツールの `manage-test-connection-blacklist` コマンドを使用して、内部ホストへのアクセスをブロックします。

■ すべてのアクティブ セルの FIPS ステータスの表示

VMware Cloud Director 10.2.2 以降で、すべてのアクティブな VMware Cloud Director セルの FIPS ステータスを確認するには、`fips-status` コマンドを使用します。このコマンドを使用しても、VMware Cloud Director アプライアンスの FIPS ステータスは表示されません。

■ 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

セルが提供する SSL プロトコルのセットの中から SSL ハンドシェイク プロセスで使用するものを構成するには、セル管理ツールの `ssl-protocols` コマンドを使用します。

■ メトリックの収集と公開の構成

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構成することができます。

■ 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

VMware Cloud 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、VMware Cloud 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。

■ メール テンプレートの構成

メール アラートの作成時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-vm` コマンドを使用すると、vCenter データベースには存在するが VMware Cloud 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 カスタム エクスぺリエンス改善プログラムへの参加または離脱

VMware カスタム エクスぺ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atalog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。

■ VMware Cloud 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

VMware Cloud Director 環境内の VMware Cloud 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 VMware Cloud 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。

■ VMware Cloud Director セルのデータベース IP アドレスの更新

データベース高可用性クラスタ内の VMware Cloud Director セルの IP アドレスを更新するには、セル管理ツールを使用できます。

VMware Cloud 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。

VMware Cloud 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 VMware Cloud 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 5-1. 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、VMware Cloud 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、VMware Cloud Director データベースに格納されます。
--installation-id	1 ～ 63 の整数	この VMware Cloud 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。 注： マルチサイト展開の VMware Cloud 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 VMware Cloud 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。
--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、VMware Cloud 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。VMware Cloud Director の有効なシリアル番号であることが必要です。
--system-name	VMware Cloud Director vCenter Server フォルダの名前。	この VMware Cloud 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。

表 5-1. セル管理ツールのオプションと引数、system-setup サブコマンド（続き）

オプション	引数	説明
--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、VMware Cloud Director の認証を受ける際に、このユーザー名を入力します。

例：VMware Cloud Director システム設定を指定する

この例のコマンドでは、VMware Cloud 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@cell11 /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.
```

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

VMware Cloud 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 VMware Cloud Director へのアクセスに、個別の VMware Cloud Director OpenAPI ログイン エンドポイントを使用できます。

2 台の新しい OpenAPI エンドポイントを使用して VMware Cloud Director へのアクセスを制限することにより、セキュリティを向上させることができます。

- /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 VMware Cloud 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 VMware Cloud 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 VMware Cloud 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。

注： サービス プロバイダによる `/api/sessions` API エンドポイントへのアクセスを無効にすると、認証ヘッダーで SAML トークンのみを指定するサービス プロバイダの要求は、すべてのレガシー API エンドポイントで失敗します。

手順

- 1 いずれかの VMware Cloud 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 VMware Cloud 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、VMware Cloud 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-usysadmin-username -p sysadmin-passwordoption
```

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 5-2. 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
<code>--help</code> (-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。
<code>--pid</code> (-i)	セル プロセスのプロセス ID	このオプションは <code>-username</code> の代わりに使用できます。
<code>--maintenance</code> (-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。
<code>--password</code> (-p)	VMware Cloud Director システム管理者のパスワード	<code>-username</code> 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。
<code>--quiesce</code> (-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。
<code>--shutdown</code> (-s)	なし	サーバ上の VMware Cloud Director サービスを正常にシャットダウンします。
<code>--status</code> (-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。
<code>--status-verbose</code> (-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。
<code>--username</code> (-u)	VMware Cloud Director システム管理者のユーザー名	このオプションは <code>-pid</code> 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。

VMware Cloud Director は VMware Cloud 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、VMware Cloud 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

VMware Cloud Director システム管理者のユーザー名。

sysadmin-password

VMware Cloud 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 VMware Cloud 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 5-3. 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>-p</code> および <code>-p</code> の代わりに使用できます。

表 5-3. セル管理ツールのオプションと引数、cell-application サブコマンド（続き）

コマンド	引数	説明
--list	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。
--password (-p)	VMware Cloud 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。
--set	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、--enable または --disable を使用します。
--username (-u)	VMware Cloud Director 管理者 ユーザー名。	--pid 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@cell11 /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、VMware Cloud Director データベースの接続プロパティを更新できます。

VMware Cloud Director のインストール プロセスまたは VMware Cloud 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構成します。[Linux への VMware Cloud Director のインストール](#)および [VMware Cloud Director アプライアンスのデプロイと初期構成](#)を参照してください。

VMware Cloud 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 VMware Cloud 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、「[Linux への VMware Cloud 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 5-4. 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
--help (-h)	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。
--database-host (-dbhost)	VMware Cloud 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	database.jdbcUrl プロパティの値を更新します。 重要： このコマンドは、値の形式のみを検証します。
--database-instance (-dbinstance)	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 sqlserver の場合に使用します。 重要： 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。
--database-name (-dbname)	データベース サービス名。	database.jdbcUrl プロパティの値を更新します。
--database-password (-dbpassword)	データベース ユーザーのパスワード。	database.password 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。
--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。	database.jdbcUrl プロパティの値を更新します。 重要： このコマンドは、値の形式のみを検証します。
--database-type (-dbtype)	データベース タイプ。次のいずれか： ■ sqlserver ■ postgres	database.jdbcUrl プロパティの値を更新します。

表 5-4. 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
--database-user (-dbuser)	データベース ユーザーの ユーザー名	database.user プロパティの値を更新 します。
--database-ssl	true または false	データベース タイプが postgres の場 合に使用します。VMware Cloud Director からの SSL 接続を要求するよ うに、PostgreSQL データベースを構成 します。
--pid (-i)	セルのプロセス ID。	オプション。実行中の VMware Cloud 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。 --private-key-path 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。
--private-key-path	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。 重要： 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。
--remote-sudo-user	sudo 権限を持つユーザー の名前。	リモート ユーザーが root と異なる場合 に、--private-key-path 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、postgres ユー ザーにこのオプションを使用できます (--remote-sudo- user=postgres 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： VMware Cloud Director プロセスを実行する ID として使用するため、VMware Cloud 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：VMware Cloud Director データベースのユーザー名とパスワードを変更する

VMware Cloud 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@55w0rd
```

例：すべてのセルのホット再構成による VMware Cloud 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 VMware Cloud Director データベースの IP アドレスを直接に変更するには、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

VMware Cloud 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-tool fix-scheduler-data options
```

表 5-5. 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	VMware Cloud 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	VMware Cloud 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。

HTTPS 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、HTTPS 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 VMware Cloud 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 HTTPS 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。HTTPS サービスのエンドポイントでは、VMware Cloud Director Service Provider Admin Portal、VMware Cloud Director Tenant Portal、および VMware Cloud Director 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 VMware Cloud 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 5-6. 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</i> [, <i>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	HTTPS エンドポイントの証明書を生成します。

表 5-6. 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
--type (-t)	<i>keystore-type</i>	キーストアの形式。デフォルトは、PKCS12 です。JCEKS キーストアを作成することもできます。
--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 HTTPS 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。HTTPS 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。VMware Cloud 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。

HTTPS 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、HTTPS 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、PKCS12 または JCEKS 形式の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に置き換えます。署名付き証明書を保存するキーストアを作成するには、[Linux 上での VMware Cloud 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 5-7. 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>--https (-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 PKCS12 または JCEKS 形式のキーストアのフル パス名です。-k に置き換えられる非推奨の -s 短縮形
<code>--keystore-password (-w)</code>	<i>keystore-password</i>	--keystore オプションによって参照される PKCS12 または JCEKS 形式のキーストアのパスワードです。非推奨の -kspassword および --keystorepwd 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@cell11 /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 VMware Cloud 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、VMware Cloud 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 5-8. 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 VMware Cloud Director ローカル キーストアにインポートします。VMware Cloud 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
```

vSphere リソースからのエンドポイント証明書のインポート

アップグレード後、セル管理ツールの `trust-infra-certs` コマンドを使用して、環境内の vSphere リソースから VMware Cloud Director データベースに証明書を収集してインポートします。

セル管理ツールの `trust-infra-certs` コマンドは、環境内の vSphere リソースから SSL 証明書を自動的に収集し、VMware Cloud Director データベースにインポートします。

前提条件

エンドポイントをインポートする vCenter Server と NSX Manager インスタンスが実行中であることを確認します。

手順

- 1 VMware Cloud 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 次の形式でコマンドを実行します。

```
/opt/vmware/vcloud-director/bin/cell-management-tool trust-infra-certs options
```

表 5-9. セル管理ツールのオプションと引数、`trust-infra-certs` 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>--vsphere</code>	なし	このインストール内の登録されているすべての vCenter Server、NSX Data Center for vSphere、および NSX-T Data Center インスタンスの証明書を信頼するように求めるメッセージが表示されます。
<code>--trust</code>	なし	オプション。VMware Cloud Director トラストストアに証明書を追加します。

表 5-9. セル管理ツールのオプションと引数、trust-infra-certs サブコマンド（続き）

オプション	引数	説明
--inspect	オプション。ファイルのパス。	オプション。証明書をファイルに表示します。
--unattended	なし	オプション。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。すべてのインフラストラクチャ証明書が自動的に信頼されます。

例：vSphere リソース エンドポイントからのすべての証明書を信頼してインポートする

追加の入力を求められることなく vSphere リソース エンドポイントからの証明書を信頼してインポートするには、次のオプションを指定してコマンドを実行します。

```
/opt/vmware/vcloud-director/bin/cell-management-tool trust-infra-certs --vsphere --unattended
```

テスト接続拒否リストの構成

インストールまたはアップグレード後、VMware Cloud Director ネットワークへのアクセスをテナントに許可する前に、セル管理ツールの `manage-test-connection-blacklist` コマンドを使用して、内部ホストへのアクセスをブロックします。

VMware Cloud Director 10.1 以降では、サービス プロバイダとテナントは VMware Cloud Director API を使用して、リモート サーバへの接続をテストし、SSL ハンドシェイク中にサーバ ID を検証できます。

VMware Cloud Director インスタンスが展開されている内部ネットワークを悪意のある攻撃から保護するために、システム プロバイダはテナントにアクセスできない内部ホストの拒否リストを構成することができます。

この方法では、テナントへのアクセス権を持つ悪意のある攻撃者が VMware Cloud Director API の接続テストを使用して VMware Cloud Director がインストールされたネットワークのマッピングを試行しても、拒否リストの内部ホストには接続できません。

インストールまたはアップグレード後、VMware Cloud Director ネットワークへのアクセスをテナントに許可する前に、セル管理ツールの `manage-test-connection-blacklist` コマンドを使用して、内部ホストに対するテナントのアクセスをブロックします。

手順

- 1 VMware Cloud 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 コマンドを実行して、拒否リストにエントリを追加します。

```
/opt/vmware/vcloud-director/bin/cell-management-tool manage-test-connection-blacklist  
option
```

表 5-10. セル管理ツールのオプションと引数、manage-test-connection-blacklist 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。
--add-ip	IPv4 または IPv6 アドレス	IP アドレスを拒否リストに追加します。
--add-name	ホストのサブドメインまたは完全修飾ドメイン名	サブドメインまたはドメイン名を拒否リストに追加します。
--add-range	CIDR またはハイフン区切り形式の IPv4 または IPv6 アドレス範囲	IP アドレス範囲を拒否リストに追加します。
--list	なし	アクセスが拒否されている既存のエントリをすべてリストします。

すべてのアクティブ セルの FIPS ステータスの表示

VMware Cloud Director 10.2.2 以降で、すべてのアクティブな VMware Cloud Director セルの FIPS ステータスを確認するには、`fips-status` コマンドを使用します。このコマンドを使用しても、VMware Cloud Director アプライアンスの FIPS ステータスは表示されません。

Linux で VMware Cloud Director の FIPS モードを有効にする方法については、VMware Cloud Director Service Provider Admin Portal Guide の [FIPS モードの有効化](#) を参照してください。

`fips-status` コマンドは、セル名、UUID、IP アドレス、FIPS ステータスなど、すべてのアクティブ セルの FIPS ステータス情報を表示します。

アプライアンス FIPS モードの詳細については、[VMware Cloud Director アプライアンス FIPS モードの表示](#) を参照してください。

JSON 形式でデータを受信するには、`--json` フラグを指定します。

手順

- 1 VMware Cloud Director 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 すべてのアクティブ セルの FIPS ステータスを表示します。

```
/opt/vmware/vcloud-director/bin/cell-management-tool fips-status
```

表 5-11. セル管理ツールのオプションと引数、fips-status 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。
--json	なし	情報を JSON 形式で表示します。

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。

注： `ciphers` コマンドは、VMware Cloud Director が HTTPS およびコンソール プロキシの通信に使用する証明書のセットにのみ適用され、VMware Cloud Director アプライアンスがアプライアンス管理ユーザー インターフェイスおよび API に使用する証明書には適用されません。

クライアントが VMware Cloud 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。

VMware Cloud 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립トがセルの証明書を調べます。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た証明書がある場合、インストールまたはアップグレードは失敗します。次の手順を実行して証明書を置き換えて、許可暗号リストを再構成できます。

- 1 禁止された暗号をいずれも使用しない証明書を作成します。以下の例に示された `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するために必要なすべての暗号を含めることができます。

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、VMware Cloud 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 5-12. 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	VMware Cloud Director でサポートされているすべての暗号を一覧表示します。
<code>--compatible-reset (-c)</code> (廃止)	なし	廃止されました。 <code>--reset</code> オプションを使用して、デフォルトの許可暗号リストにリセットします。

表 5-12. 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>--disallow (-d)</code>	暗号名のカンマ区切りのリスト	<p>指定されたカンマ区切りリストで暗号を禁止します。このオプションを実行すると前の設定が上書きされるため、このオプションを実行するたびに、無効にする暗号の完全なリストを含める必要があります。</p> <p>重要： 値を指定せずにオプションを実行すると、すべての暗号が有効になります。</p> <p>使用可能なすべての暗号を表示するには、<code>-a</code> オプションを指定して実行します。</p> <p>重要： <code>ciphers --disallow</code> を実行した後に、セルを再起動する必要があります。</p>
<code>--list (-l)</code>	なし	現在使用している許可された暗号セットを一覧表示します。
<code>--reset (-r)</code>	なし	<p>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。</p> <p>重要： <code>ciphers --reset</code> を実行した後に、セルを再起動する必要があります。</p>

例：2 つの暗号の禁止

VMware Cloud Director には、事前設定された有効な暗号のリストが含まれています。

この例では、許可暗号リストから追加の暗号を有効にする方法、および使用しない暗号を禁止する方法を示します。

- 1 デフォルトで有効になっている暗号のリストを取得します。

```
[root@cell11 /opt/vmware/vcloud-director/bin]# ./cell-management-tool ciphers -l
```

このコマンドの出力では有効な暗号のリストが返されます。

```
Allowed ciphers:
* TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
* TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
* TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
* TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
```

- 2 SSL ハンドシェイク中にセルが提供できるすべての暗号のリストを取得します。

```
[root@cell11 /opt/vmware/vcloud-director/bin]# ./cell-management-tool ciphers -a
```

このコマンドの出力では許可暗号リストが返されます。

```
# ./cell-management-tool ciphers -a
Product default ciphers:
* TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
* TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
* TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
* TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
* TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
* TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
* TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
* TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
* TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
* TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
* TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
* TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
* TLS_RSA_WITH_AES_256_GCM_SHA384
* TLS_RSA_WITH_AES_128_GCM_SHA256
* TLS_RSA_WITH_AES_256_CBC_SHA256
* TLS_ECDH_RSA_WITH_AES_256_CBC_SHA
* TLS_RSA_WITH_AES_256_CBC_SHA
* TLS_RSA_WITH_AES_128_CBC_SHA256
* TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA
* TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA
* TLS_ECDH_RSA_WITH_AES_128_CBC_SHA
* TLS_RSA_WITH_AES_128_CBC_SHA
```

3 無効にする暗号を指定します。

このコマンドを実行して暗号を明示的に無効にしない場合は、暗号が有効になります。

```
[root@cell11 /opt/vmware/vcloud-director/
bin]# ./cell-management-tool ciphers -d
TLS_RSA_WITH_AES_128_CBC_SHA,TLS_ECDH_RSA_WITH_AES_128_CBC_SHA
```

4 コマンドを実行して、有効な暗号のリストを確認します。リストにない暗号は無効です。

```
root@bos1-vcd-static-211-90 [ /opt/vmware/vcloud-
director/bin ]# ./cell-management-tool ciphers -l
```

この出力では、現在有効になっているすべての暗号のリストが返されます。

```
Allowed ciphers:
* TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
* TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
* TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
* TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
* TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
* TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
* TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
* TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
* TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
* TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
* TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
```

```
* TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
* TLS_RSA_WITH_AES_256_GCM_SHA384
* TLS_RSA_WITH_AES_128_GCM_SHA256
* TLS_RSA_WITH_AES_256_CBC_SHA256
* TLS_ECDH_RSA_WITH_AES_256_CBC_SHA
* TLS_RSA_WITH_AES_256_CBC_SHA
* TLS_RSA_WITH_AES_128_CBC_SHA256
* TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA
* TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA
```

許可された SSL プロトコルのリストの管理

セルが提供する SSL プロトコルのセットの中から SSL ハンドシェイク プロセスで使用するものを構成するには、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 VMware Cloud 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、および SSLv2Hello を含む一部のプロトコルは、既知のセキュリティ上の重大な脆弱性があるため、デフォルトのリストには含まれていません。

手順

- 1 VMware Cloud Director 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 次のコマンドを実行して、許可された SSL プロトコルのリストを管理します。

```
cell-management-tool ssl-protocols options
```

表 5-13. 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	VMware Cloud Director でサポートされるすべての SSL プロトコルを一覧表示します。

表 5-13. セル管理ツールのオプションと引数、`ssl-protocols` サブコマンド（続き）

オプション	引数	説明
<code>--disallow (-d)</code>	SSL プロトコル名のコンマ区切りのリスト	<p>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。このオプションを実行すると前の設定が上書きされるため、このオプションを実行するたびに、無効にする SSL プロトコルの完全なリストを含める必要があります。</p> <p>重要： 値を指定せずにオプションを実行すると、すべての SSL プロトコルが有効になります。</p> <p>使用可能なすべての SSL プロトコルを表示するには、<code>-a</code> オプションを指定して実行します。</p> <p>重要： <code>ssl-protocols --disallow</code> を実行した後に、セルを再起動する必要があります。</p>
<code>--list (-l)</code>	なし	現在使用している許可された SSL プロトコル セットを一覧表示します。
<code>--reset (-r)</code>	なし	<p>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。</p> <p>重要： <code>ssl-protocols --reset</code> を実行した後に、セルを再起動する必要があります。</p>

例：許可された SSL プロトコルと構成された SSL プロトコルの一覧表示、および許可されていない SSL プロトコルのリストの再構成

`--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@cell11 /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@cell11 /opt/vmware/vcloud-director/bin]# ./cell-management-tool ssl-protocols -l
Allowed SSL protocols:
```

```
* TLSv1.2
* TLSv1.1
```

許可されていない SSL プロトコルのリストを再構成するには、`--disallow (-d)` オプションを使用します。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 vCenter Server リリースには TLSv1 が必要です。

```
[root@cell11 /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に、セルを再起動する必要があります。

メトリックの収集と公開の構成

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構成することができます。

VMware Cloud Director は、仮想マシンのパフォーマンスおよびリソース使用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、VMware Cloud Director によって収集されるメトリックを構成します。`cell-management-toolcassandra` サブコマンドを使用して、VMware Cloud Director メトリック リポジトリとして使用するための Apache Cassandra データベースを構成します。

[Cassandra メトリック データベースの構成](#)を参照してください。

手順

- 1 VMware Cloud Director 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 VMware Cloud Director が収集するメトリックを構成します。

```
/opt/vmware/vcloud-director/bin/cell-management-tool configure-metrics --metrics-config
pathname
```

表 5-14. 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
<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>--repository-host</code> (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。 <code>cell-management-tool cassandra</code> サブコマンドの <code>--cluster-nodes</code> オプションを使用して、VMware Cloud Director メトリック リポジトリとして使用するための Apache Cassandra データベースを構成します。

表 5-14. セル管理ツールのオプションと引数、configure-metrics サブコマンド（続き）

コマンド	引数	説明
--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、VMware Cloud Director メトリック リポジトリとして使用するための Apache Cassandra データベースを構成します。
--metrics-config	パス名	メトリック構成ファイルのパス

- 3 VMware Cloud Director のバージョンが 10.2.2 以降の場合は、次のコマンドを実行してメトリックの公開を有効にすることもできます。

```
/opt/vmware/vcloud-director/bin/cell-management-tool manage-config -n
statsFeeder.metrics.publishing.enabled -v true
```

VMware Cloud Director 10.2.2 以降では、メトリックの公開はデフォルトで無効です。

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、メトリック収集を構成します。

```
[root@cell11 /opt/vmware/vcloud-director/
bin]# ./cell-management-tool configure-metrics --metrics-config /tmp/metrics.groovy
```

VMware Cloud 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 5-15. 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、VMware Cloud Director はメトリックをすべてのディスクの集計として報告します。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 5-16. 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）。デフォルト値は 20 です。vSphere Performance Manager の定義に従い、VMware Cloud Director で 20 を超える値がサポートされるのは、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。デフォルト値は 20 です。vSphere Performance Manager の定義に従い、VMware Cloud Director で 20 を超える値がサポートされるのは、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	メトリックが使用可能な vCenter Server オブジェクトのタイプ。デフォルトは、VM です。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 コア数）、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。デフォルトは、"*" です。

表 5-16. 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。つまり、レポート間隔は確保されません。
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。デフォルトは、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。

VMware Cloud 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、VMware Cloud 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。[メトリックの収集と公開の構成](#)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。

VMware Cloud 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 5-17. 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。 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。
<code>--cluster-nodes</code>	<code>address [, address ...]</code>	VMware Cloud 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 VMware Cloud Director データベースから削除します。

表 5-17. 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
--configure	なし	既存の Cassandra クラスタで使用する VMware Cloud Director を構成します。
--dump	なし	現在の接続の設定をダンプします。
--keyspace	文字列	Cassandra の VMware Cloud 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 <code>vcloud_metrics</code> です。
--offline	なし	VMware Cloud Director で使用するために Cassandra を設定しますが、VMware Cloud 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 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	VMware Cloud 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@cell11 /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

VMware Cloud 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、VMware Cloud 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、VMware Cloud 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、VMware Cloud 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 5-18. 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
<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>--dbuser</code>	VMware Cloud 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。
<code>--dbpassword</code>	VMware Cloud 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 5-19. 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
<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>--message (-m)</code>	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@cell11 /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 VMware Cloud Director セル内のサービスは、監査メッセージを VMware Cloud 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 VMware Cloud 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 VMware Cloud 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。『VMware Cloud Director インストール、構成、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 5-20. 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
--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 (-d)	なし	ログの作成を syslog への監査イベントについて無効にします。監査イベントを VMware Cloud 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、global.properties および responses.properties の audit.syslog.host および audit.syslog.port プロパティの値が設定解除されます。
--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	このオプションを指定すると、audit.syslog.host 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。
--syslog-port (-logport)	0～65535 の整数	このオプションを指定すると、audit.syslog.port 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。『VMware Cloud Director インストール、構成、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利用」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@cell11 /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。

メール テンプレートの構成

メール アラートの作成時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。

デフォルトでは、システムは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メール アラートを送信するように構成されています。E メールを受信者リストは、VMware Cloud Director 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 5-21. 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
<code>--help</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>--delete</code>	テンプレート名	削除するテンプレートの名前。
<code>--lookup</code>	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。
<code>--locale</code>	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。別のロケールを指定するには、このオプションを使用します。
<code>--set-template</code>	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 <code>vcloud.vcloud</code> によって読み取り可能である必要があります。例: <code>/tmp/my-email-template.txt</code>

いくつかの許可済みのテンプレート名をさまざまな E メール通知に使用できます。

表 5-22. VMware Cloud Director の E メール通知名

名前	説明	E メールが送信されるタイミング	受信者
<code>VAPP_UNDEPLOY_NOTIFICATION_BODY</code>	vApp のランタイム リースの期限切れが近くなるとアラートを生成します。リースが期限切れになると、VMware Cloud Director が vApp をサスペンドまたはパワーオフします。	構成された展開およびストレージ リース アラート時間に依拠して決まる、vApp のランタイム リースが期限切れになる前の時点。	vApp の所有者、または所有者がシステム管理者である場合は組織管理者が通知を受信します。
<code>VAPP_STORAGE_NOTIFICATION_BODY</code>	vApp のストレージ リースの有効期限が近くなるとアラートを生成します。リースが期限切れになると、VMware Cloud Director が vApp を削除します。	構成された展開およびストレージ リース アラート時間に依拠して決まる、vApp のストレージ リースが期限切れになる前の時点。	vApp の所有者、または所有者がシステム管理者である場合は組織管理者が通知を受信します。

表 5-22. VMware Cloud Director の E メール通知名 (続き)

名前	説明	E メールが送信されるタイミング	受信者
VAPP_STORAGE_NOTIFICATION_BODY	vApp のストレージ リースの有効期限が近くなるとアラートを生成します。リースが期限切れになると、VMware Cloud Director が vApp を期限切れとマークします。	構成された展開およびストレージ リース アラート時間に応じて決まる、vApp のストレージ リースが期限切れになる前の時点。	vApp の所有者、または所有者がシステム管理者である場合は組織管理者が通知を受信します。
VAPPTEMPLATE_STORAGE_NOTIFICATION_BODY	vApp テンプレートのストレージ リースの有効期限が近くなるとアラートを生成します。リースが期限切れになると、VMware Cloud Director が vApp テンプレートを削除します。	構成された展開およびストレージ リース アラート時間に応じて決まる、vApp テンプレートのストレージ リースが期限切れになる前の時点。	vApp テンプレートの所有者、または所有者がシステム管理者である場合は組織管理者が通知を受信します。
VAPPTEMPLATE_STORAGE_NOTIFICATION_BODY	vApp テンプレートのストレージ リースの有効期限が近くなるとアラートを生成します。リースが期限切れになると、VMware Cloud Director が vApp テンプレートを期限切れとマークします。	構成された展開およびストレージ リース アラート時間に応じて決まる、vApp テンプレートのストレージ リースが期限切れになる前の時点。	vApp テンプレートの所有者、または所有者がシステム管理者である場合は組織管理者が通知を受信します。
DISK_STORAGE_ALERT	ディスク ストレージ アラート (レッド アラート)	データストアのディスク容量が少なくなり、赤しきい値に達したとき。	システム管理者
DISK_STORAGE_ALERT_VDCS	プロバイダ VDC に対するディスク ストレージ アラート。E メールには、ハード ディスクの容量不足が原因でレッド アラートが表示されているデータストアを使用しているプロバイダ VDC のリストが含まれています。	データストアのディスク容量が少なくなり、赤しきい値に達したとき。	システム管理者
VM_HW_UPGRADE_INVALID_POWERSTATE	仮想マシンの電源状態に関する通知。仮想ハードウェアをアップグレードするに際し、仮想マシンをパワーオフする必要があります。	ユーザーが仮想マシン ハードウェアのバージョンのアップグレードを試行したとき。	仮想マシンの所有者、または所有者がシステム管理者である場合は組織管理者が通知を受信します。
FEDERATION_CERTIFICATE_SUCCESS	外部 SSO サーバの証明書の有効期限が近くなると、すべての組織管理者に送信される連携証明書の有効期限通知。これにより、組織管理者は SSO サーバから新しい証明書をダウンロードして VMware Cloud Director を更新するように求められます。	連携証明書が現在の日付から 7 日以内に期限切れになるとき。	組織管理者
IPSEC_VPN_TUNNEL_ERROR	VPN トンネル エラー (レッド アラート)	VPN トンネルが動作していない場合。	システム管理者
IPSEC_VPN_TUNNEL_ERROR_SUMMARY			

表 5-22. VMware Cloud Director の E メール通知名（続き）

名前	説明	E メールが送信されるタイミング	受信者
IPSEC_VPN_TUNNEL_ENABLED	VPN トンネルが有効（グリーンアラート）	動作しなくなった VPN トンネルが再び動作するようになったとき。	システム管理者
IPSEC_VPN_TUNNEL_ENABLED_SUMMARY			

表 5-23. カスタマイズできないメール テンプレート

通知	E メールが送信されるタイミング	受信者
再接続された vCenter Server のメール アラート	vCenter Server が再接続されたとき。	システム管理者
切断された vCenter Server のメール アラート。この E メールには、エラーとユーザー要求のどちらによって vCenter Server の切断が発生したかが記載されます。	vCenter Server が切断されたとき。	システム管理者
AMQP 接続切断のメール アラート。VMware Cloud Director が AMQP サーバから切断されたことを通知するアラートです。	RabbitMQ が動作を停止したとき。	システム管理者
データベース接続の切断に関するメール アラート	VMware Cloud Director がデータベースから切断されたとき。	システム管理者
データベース接続の復元に関するメール アラート	VMware Cloud Director がデータベースに再接続されたとき。	システム管理者
ホストがスイッチから切断されたことに関するメール アラート	使用可能なスイッチからホストが切断されたとき。	システム管理者
ホストが Distributed Switch から切断されたことに関するメール アラート	使用可能な Distributed Switch からホストが切断されたとき。	システム管理者
LDAP エラーのメール アラート	LDAP との同期中。	システム管理者
LDAP ユーザー同期のメール アラート	LDAP ユーザーの名前変更時。	システム管理者
サイトの関連付けステータス変更のメール アラート	最近、サイトとの接続が切断されたか、接続が回復したか、またはサイトが引き続き停止しています。	システム管理者

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@cell11 /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): $pvdcsList
"

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, pvdcsList]
  template content     : This is an alert from $productName The $datastore is used by the
followingProvider VDC(s): $pvdcsList
```

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 VMware Cloud 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、VMware Cloud 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 VMware Cloud 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、VMware Cloud 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 VMware Cloud Director または vCenter Server 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-vms options
```

表 5-24. セル管理ツールのオプションと引数、`find-orphan-vms` 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>--enableVerifyHostname</code>	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。
<code>--host</code>	必須	親なしの仮想マシンの検索対象となる VMware Cloud 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。
<code>--output-file</code>	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。
<code>--password (-p)</code>	必須	VMware Cloud Director システム管理者のパスワード。

表 5-24. セル管理ツールのオプションと引数、find-orphan-vmns サブコマンド（続き）

オプション	引数	説明
--port	VMware Cloud Director の HTTPS ポート。	このオプションは、デフォルトの VMware Cloud 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 VMware Cloud 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	VMware Cloud 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@cell11 /opt/vmware/vcloud-director/bin]# ./cell-management-tool find-orphan-vmns \
--host 10.20.30.40 -u vcadmin -vc-name vcenter1 -vc-password P@55w0rd --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 5-25. 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
<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>--disable</code>	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。
<code>--enable</code>	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。
<code>--status</code>	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@cell11 /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@cell11 /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 5-26. 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
<code>--help(-h)</code>	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。
<code>--delete(-d)</code>	なし	ターゲットの設定を削除します。
<code>--lookup(-l)</code>	なし	ターゲットの設定の値を検索します。
<code>--name(-n)</code>	設定名	ターゲットの設定の名前。 オプション <code>-d</code> 、 <code>-l</code> 、および <code>-v</code> が必要です。
<code>--value(-v)</code>	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 VMware Cloud 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 5-27. 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>VMware Cloud 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 VMware Cloud 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>VMware Cloud 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>VMware Cloud 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>VMware Cloud 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ス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@cell11 /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。

VMware Cloud 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

VMware Cloud Director 環境内の VMware Cloud 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、VMware Cloud Director Service Provider Admin Portal または VMware Cloud 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

VMware Cloud 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 VMware Cloud 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、VMware Cloud 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。

アプライアンス環境のセル設定中に、VMware Cloud 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 VMware Cloud 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、VMware Cloud 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、VMware Cloud 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 5-28. 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@cell11 /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 VMware Cloud 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。

VMware Cloud 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。VMware Cloud 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 VMware Cloud 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 VMware Cloud Director メンバーから実行します。このコマンドは VMware Cloud 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、VMware Cloud 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 5-29. 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
<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>--regenerate</code>	なし	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。 注： 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、 セルの管理 を参照してください。

表 5-29. 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（続き）

オプション	引数	説明
--regenerate-with-seed	0 ～ 63 のシード番号	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。 注： 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、 セルの管理 を参照してください。
--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、『VMware Cloud 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@cell11 /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@cell11 /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。

VMware Cloud Director セルのデータベース IP アドレスの更新

データベース高可用性クラスタ内の VMware Cloud Director セルの IP アドレスを更新するには、セル管理ツールを使用できます。

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 アドレスを調べるには、VMware Cloud Director アプライアンス API を使用して、クラスタ内のスタンバイ ノードのノード ID をメモする必要があります。<http://code.vmware.com> の「VMware Cloud Director アプライアンス API スキーマ リファレンス」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 として直接、または SSH クライアントを使用してログインします。
- 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、VMware Cloud Director セルは実行されており、VMware Cloud 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 VMware Cloud 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ことを確認します。

```
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
```

VMware Cloud Director ログの収集

6

VMware Cloud Director は、サーバ グループ内の各クラウド セルのログ情報を提供します。ログを表示してセルを監視し、VMware Cloud Director の日常的な実行中に発生した問題のトラブルシューティングを行うことができます。

VMware Cloud Director ログ

ログ名ファイルまたはディレクトリ	説明
/opt/vmware/vcloud-director/logs/cell.log	VMware Cloud Director セルからのコンソール出力。
/opt/vmware/vcloud-director/logs/cell-management-tool	セルからのセル管理ツール ログ メッセージ。
/opt/vmware/vcloud-director/logs/cell-runtime	セルからのランタイム ログ メッセージ。
/opt/vmware/vcloud-director/logs/cloud-proxy	セルからのクラウド プロキシ ログ メッセージ。
/opt/vmware/vcloud-director/logs/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。
/opt/vmware/vcloud-director/logs/server-group-communications	セルからのサーバ グループ通信。
/opt/vmware/vcloud-director/logs/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。
/opt/vmware/vcloud-director/logs/vcloud-container-debug.log	セルからのデバッグ レベルのログ メッセージ。
/opt/vmware/vcloud-director/logs/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。
/opt/vmware/vcloud-director/logs/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。セルが応答を停止した時刻や再起動した時刻などが記録されます。
/opt/vmware/vcloud-director/logs/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。
/opt/vmware/vcloud-director/logs/YYYY_MM_DD.request.log	Apache 共通ログ形式の HTTP 要求ログ。

VMware Cloud Director アプライアンスのログ

VMware Cloud Director アプライアンスには、いくつかの追加のログ ファイルがあります。

ログ ファイル	説明
/opt/vmware/var/log/firstboot	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	Replication Manager (repmgr) ツール スイートのセットアップ、再構成、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	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	OVF デプロイ パラメータが含まれています。
/var/vmware/vpostgres/current/pgdata/log	組み込み PostgreSQL データベースに関連するログが含まれています。
/opt/vmware/var/log/vami/updatecli.log	アプライアンスのアップグレードに関連するログが含まれています。

任意のテキスト エディタ、テキスト ビューア、またはサードパーティ製ツールを使用してログを表示します。

VMware Cloud Director ソフトウェアのアンインストール

7

個々のサーバーから VMware Cloud 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-phonhome 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、VMware Cloud 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。