vCloud Director インストールおよびアップグレード ガイド

vCloud Director 8.0

このドキュメントは新しいエディションに置き換わるまで、ここで書いてある各製品と後続のすべてのバージョンをサポートします。このドキュメントの最新版をチェックするには、http://www.vmware.com/jp/support/pubs を参照してください。

JA-001716-00

vmware®

最新の技術ドキュメントは VMware の Web サイト（http://www.vmware.com/jp/support/）にあります
VMware の Web サイトでは最新の製品アップデートも提供されています。
このドキュメントに関するご意見およびご感想がある場合は、docfeedback@vmware.com までお送りください。

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

ヴイエムウェア株式会社
105-0013　東京都港区浜松町 1-30-5
浜松町スクエア 13F
www.vmware.com/jp

目次

VMware vCloud Director インストールおよびアップグレード ガイド

『VMware vCloud Director インストールおよびアップグレード ガイド』には、VMware® vCloud Director® ソフトウェアをインストールまたはアップグレードし、VMware vCenter™ と連携して VMware 対応の VMware vCloud® サービスを提供するように構成する方法が記載されています。

対象読者

『VMware vCloud Director インストールおよびアップグレード ガイド』は、VMware vCloud Director ソフトウェアをインストールまたはアップグレードするユーザーを対象としています。本書の情報は、Linux、Windows、IP ネットワーク、および VMware vSphere® に精通した、経験の豊富なシステムの管理者向けに記載されています。

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

1

VMware vCloud® では、vCloud Director サーバー グループを vSphere プラットフォームと統合します。vCloud Director サーバー グループを作成するには、vCloud Director ソフトウェアを 1 つ以上のサーバーにインストールし、それらのサーバーを共有データベースに接続して、vCloud Director サーバー グループを vSphere と統合します。

データベースとネットワーク接続の詳細を含む vCloud Director の初期構成は、インストール時に確立されます。インストールされている既存の vCloud Director を新しいバージョンにアップグレードする場合は、vCloud Director ソフトウェアとデータベース スキーマをアップデートし、サーバー、データベース、および vSphere 間の既存の関係はそのまま残します。

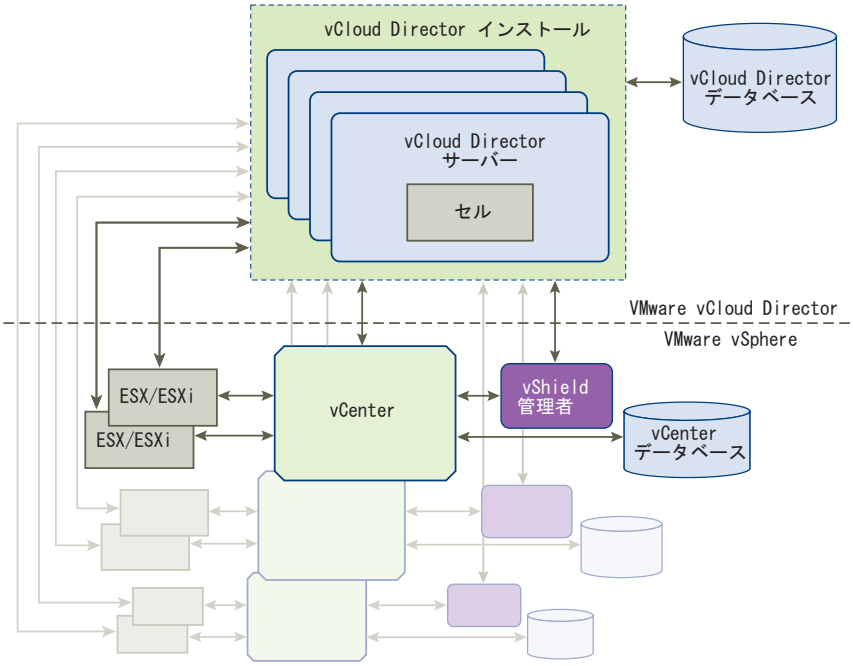
この章では次のトピックについて説明します。

vCloud Director のアーキテクチャ

vCloud Director サーバー グループは 1 つ以上の vCloud Director サーバーで構成されます。これらのサーバーは共通のデータベースを共有し、任意の数の vCenter Server システムおよび ESXi ホストとリンクします。ネットワーク サービスは VMware vCloud® Networking and Security™ の VMware vShield Manager™ コンポーネント、または VMware NSX™ for vSphere® の VMware NSX Manager™ コンポーネントから、vCenter Server システムおよび vCloud Director に提供されます。

標準的なインストールでは、いくつかのサーバーで構成される vCloud Director サーバー グループが作成されます。グループの各サーバーは vCloud Director セルと呼ばれる一連のサービスを実行します。グループ内のすべてのメンバーは 1 つのデータベースを共有します。グループ内の各セルは複数の vCenter Server システム、これらの管理ホスト、および接続された各 vCenter Server システムをサポートするように構成された各 vShield Manager または NSX Manager に接続されます。

図 1-1. vShield Manager を使用するインストールの vCloud Director アーキテクチャ図



vCloud Director のインストールおよび構成プロセスではセルを作成し、それらを共有データベースに接続して、vCenter Server システム、その vCenter Server システムに関連付けられた vShield Manager または NSX Manager、およびそのホストとの最初の接続を確立します。その後システム管理者は vCloud Director Web コンソールを使用して vCenter Server システム、追加された vCenter Server システムに関連付けられた vShield Manager または NSX Manager、および追加された vCenter Server システムのホストを vCloud Director サーバー グループにいつでも追加できます。

構成の計画

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

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

- クラウド内でアクセス可能にする vCenter Server システムごとに 1 つの vCloud Director サーバー（セル）を割り当てます。
- すべての vCloud Director サーバーが、メモリおよびストレージの最小要件を満たしていることを確認します（「vCloud Director のハードウェアおよびソフトウェア要件 (P. 9)」を参照）。
- 「vCloud Director データベースのインストールと構成 (P. 15)」 の説明に従って vCloud Director データベースを構成します。

vCloud Director のハードウェアおよびソフトウェア要件

vCloud Director サーバー グループの各サーバーは、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。各サーバー グループには、vCenter Server、vShield Manager または NSX Manager、および 1 つ以上の ESXi ホストへのアクセス権限が必要です。

サポート対象プラットフォーム

vCloud Director の本リリースがサポートしている VMware プラットフォームに関する最新情報は、http://partnerweb.vmware.com/comp_guide/sim/interop_matrix.php の「VMware 製品の互換性マトリックス」で確認できます。

vSphere 構成要件

vCloud Director で使用するサーバーおよびホストは、特定の構成要件を満たす必要があります。

- vCloud Director の外部ネットワークまたはネットワーク プールとして使用する vCenter ネットワークは、vCloud Director で使用するクラスタ内のすべてのホストから使用できる必要があります。これらのネットワークをデータセンター内のすべてのホストから使用できるようにすることで、新しい vCenter Server を vCloud Director に追加するタスクが簡素化されます。
- ホスト間のフェンスとネットワーク プールの割り当てに vSphere Distributed Switch を使用する必要があります。
- vCenter クラスタを vCloud Director で使用する場合、自動化レベルが [完全に自動化] である Storage DRS を使用するように構成する必要があります。この構成は、DRS クラスタのすべての ESXi ホストに接続された共有ストレージを必要とします。vCloud Director では、高速プロビジョニングのサポートを含め、Storage DRS を活用できます。
- vCenter Server はホストを信頼している必要があります。vCloud Director によって管理されるすべてのクラスタのすべてのホストは、検証されたホスト証明書が必要とされるように構成する必要があります。特に、すべてのホストで一致するサムプリントを決定、比較、および選択する必要があります。『vCenter Server とホスト管理』ドキュメントの「SSL 設定の構成」を参照してください。

vSphere ライセンス要件

vCloud Director は、以下の vSphere ライセンスを必要とします。

- vSphere Enterprise および Enterprise Plus によりライセンスを付与された VMware DRS。
- vSphere Enterprise Plus によりライセンスを付与された VMware Distributed Switch および dvFilter。このライセンスは、vCloud Director の隔絶されたネットワークの作成と使用を有効にします。

サポート対象の vCloud Director サーバー オペレーティング システム

表 1-1. サポート対象の vCloud Director サーバー オペレーティング システム

オペレーティング システム (64 ビットのみ)	更新
CentOS 6	4
Red Hat Enterprise Linux 5	4-10
Red Hat Enterprise Linux 6	1-5

ディスク容量の要件

各 vCloud Director サーバーに、インストールとログ ファイル用として約 1450MB の空き容量が必要です。

メモリ要件

各 vCloud Director サーバーに、4GB 以上のメモリをプロビジョニングする必要があります。

Linux ソフトウェア パッケージ

各 vCloud Director サーバーには、数個の共通 Linux ソフトウェア パッケージがインストールされている必要があります。これらのパッケージは、通常、オペレーティング システム ソフトウェアと一緒にデフォルトでインストールされます。欠落しているパッケージがあると、インストーラは診断メッセージを表示して終了します。

表 1-2. 必須のソフトウェア パッケージ

パッケージ名	パッケージ名	パッケージ名
alsa-lib	libICE	module-init-tools
bash	libSM	net-tools
chkconfig	libstdc	pciutils
coreutils	libX11	procps
findutils	libXau	redhat-lsb
glibc	libXdmcp	sed
grep	libXext	tar
initscripts	libXi	which
krb5-libs	libXt	
libgcc	libXtst	

注意　ネットワーク接続を構成し、SSL 証明書を作成するための手順では、Linux `bind-utils` パッケージで使用可能な Linux `nslookup` コマンドを使用する必要があります。

サポート対象の vCloud Director データベース

vCloud Director は、Oracle および Microsoft SQL Server データベースをサポートしています。vCloud Director の本リリースでサポートされているデータベースの最新情報は、VMware Partner Central にある「VMware 製品の互換性マトリックス」で確認してください。VMware パートナー アカウント情報を使用して VMware Partner Central にログインします。

推奨されるデータベース サーバー構成については、「vCloud Director データベースのインストールと構成 (P. 15)」を参照してください。

サポート対象の LDAP サーバー

表 1-3. サポート対象の LDAP サーバー

プラットフォーム	LDAP サーバー	認証方式
Windows Server 2003	Active Directory	シンプル、シンプル SSL、ケルベロス、ケルベロス SSL
Windows Server 2008	Active Directory	シンプル
Windows 7 (2008 R2)	Active Directory	シンプル、シンプル SSL、ケルベロス、ケルベロス SSL
Linux	OpenLDAP	シンプル、シンプル SSL

ゲスト OS のサポート

サポートされているゲスト OS の一覧については、『VMware vCloud Director ユーザー ガイド』を参照してください。

履歴メトリック データを格納するためのサポート対象データベース

vCloud Director が仮想マシンのパフォーマンスおよびリソース消費量について収集するメトリックを格納するように vCloud Director のインストールを構成できます。履歴メトリックのデータは Cassandra でバッキングされる KairosDB データベースに格納されます。詳細については、第 6 章「過去の仮想マシン パフォーマンス メトリックを格納および取得するためのオプション データベース ソフトウェアのインストールと構成 (P. 69)」を参照してください。

vCloud Director は次の KairosDB および Cassandra バージョンをサポートしています。

- KairosDB 0.9.1
- Cassandra 1.2 および 2.0

vCloud Director のサポート対象ブラウザ

vCloud Director Web コンソールは、Google Chrome、Mozilla Firefox および Microsoft Internet Explorer の最新のバージョンと互換性があります。

注意　vCloud Director Web コンソールは、32 ビット ブラウザとのみ互換性があります。ブラウザが 64 ビット プラットフォームのサポート対象に含まれている場合、64 ビット プラットフォーム上の 32 ビット ブラウザを使用することを示します。

Linux プラットフォームでのブラウザ サポート

Linux プラットフォームでは、vCloud Director Web コンソールは、Mozilla Firefox と Google Chrome の最新バージョンおよびその直近のバージョンと互換性があります。

表 1-4. Linux プラットフォームのブラウザ サポートとオペレーティング システムの互換性

プラットフォーム	Google Chrome	Mozilla Firefox
CentOS 6<x>	はい	はい
Red Hat Enterprise Linux 6<x>	はい	はい
Ubuntu 12。<x>	はい	はい

Windows プラットフォームでのブラウザ サポート

Windows プラットフォームでは、vCloud Director Web コンソールは、Microsoft Internet Explorer の少なくとも 1 つのバージョンと互換性があります。一部の Windows プラットフォームは、Mozilla Firefox と Google Chrome の最新バージョンおよびその直近のバージョンとも互換性があります。

表 1-5. Microsoft Windows プラットフォームのブラウザ サポートとオペレーティング システムの互換性

プラットフォーム	Google Chrome	Mozilla Firefox	Internet Explorer 8.<x>	Internet Explorer 9.<x>	Internet Explorer 10.<x>
Windows XP Pro	はい	はい	はい	なし	なし
Windows Server 2003 Enterprise Edition	はい	はい	はい	なし	なし
Windows Server 2008	はい	はい	はい	はい	はい
Windows Server 2008 R2	はい	はい	はい	はい	はい
Windows Vista	はい	なし	はい	はい	はい
Windows 7	はい	はい	はい	はい	はい
Windows 8	はい	はい	なし	なし	はい

Macintosh プラットフォームでのブラウザ サポート

Macintosh プラットフォームでは、vCloud Director Web コンソールは、Mozilla Firefox と Google Chrome の最新バージョンおよびその直近のバージョンと互換性があります。

Adobe Flash Player のサポート対象バージョン

vCloud Director Web コンソールには、Adobe Flash Player 11.2 以降が必要です。32 ビット バージョンのみがサポートされています。

サポートされている Java のバージョン

vCloud Director クライアントは JRE 1.6.0 のアップデート 10 またはそれ以降をインストールし、有効にしておかなければなりません。32 ビット バージョンのみがサポートされています。

サポートされるセキュリティ プロトコルおよび暗号化スイート

vCloud Director を使用するにはクライアント接続が安全である必要があります。SSL バージョン 3 にはセキュリティ上の重大な脆弱性があることがわかっており、クライアント接続を確立するときにサーバーが提供するデフォルトのプロトコルのセットには含まれていません。次のセキュリティ プロトコルがサポートされます。

- TLS バージョン 1.0
- TLS バージョン 1.1
- TLS バージョン 1.2

`cell-management-tool` を使用してプロトコルのデフォルト セットを再構成することができます。「許可された SSL プロトコルのリストの管理 (P. 64)」 を参照してください。

サポート対象の暗号化スイートには、RSA、DSS、または楕円曲線署名に対応した暗号化方式、および DES3、AES-128、または AES-256 暗号化方式があります。`cell-management-tool` を使用してサポートされる SSL 暗号のセットを再構成することができます。「許可された SSL 暗号のリストの管理 (P. 63)」 を参照してください。

vCloud Director のネットワーク構成要件の要約

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

vCloud Director サーバ、データベース サーバー、vCenter Server、および関連付けられた vCloud Networking and Security コンポーネントまたは NSX for vSphere コンポーネントに接続するネットワークは、次の複数の要件を満たす必要があります。

IP アドレス

vCloud Director サーバーごとに、2 つの異なる SSL 接続をサポートできるように 2 つの IP アドレスが必要です。1 つの接続は HTTP サービス用です。もう 1 つの接続は、コンソール プロキシ サービス用です。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 Linux の `ip addr add` コマンドを使用することはできません。

コンソール プロキシ アドレス

コンソール プロキシ アドレスとして構成される IP アドレスは、SSL 終了ロード バランサーまたはリバース 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。

ネットワーク タイム サービス

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

サーバーのタイム ゾーン

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

ホスト名の解決

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

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

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

```
nslookup 192.168.1.1
```

転送サーバー ストレージ

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 vCloud 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できる必要があります。転送サーバー ストレージに NFS を使用する場合、vCloud Director サーバー グループの vCloud Director セルがそれぞれ NFS ベースの転送サーバー ストレージをマウントして使用できるように特定の構成を設定する必要があります。詳細については、http://kb.vmware.com/kb/2086127 を参照してください。サーバー 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（通常は `/opt/vmware/vcloud-director/data/transfer`）にマウントする必要があります。このボリュームの領域は、次の 2 通りの方法で消費されます。

- 転送 (アップロードおよびダウンロード) は、転送の進行中のみこのストレージに保管され、転送が終了すると削除されます。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ングを有効化するカタログに含まれるカタログ項目は、それが存在する限りこのストレージに保管されます(外部に公開されても、キャッシングを有効化しないカタログの項目は、このストレージに保管されません)。外部に公開されたカタログの作成をクラウド内の組織で有効化する場合は、数百あるいは数千のカタログ項目がこのボリュームの領域を必要とし、各カタログ項目が圧縮された OVF 形式の仮想マシンのサイズになると想定されます。

注意　可能であれば、転送サーバー ストレージに使用するボリュームを、容量を簡単に拡張できるボリュームにする必要があります。

ネットワーク セキュリティ要件

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

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

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

表 1-6. vCloud Director ホストからの受信パケットを許容する必要があるポート

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

- 送信接続に使用されるポートを公開ネットワークに接続しないでください。

表 1-7. vCloud Director ホストからの送信パケットを許容する必要があるポート

ポート	プロトコル	コメント
25	TCP、UDP	SMTP
53	TCP、UDP	DNS
111	TCP、UDP	転送サービスで使用される NFS ポートマッパー
123	TCP、UDP	NTP
389	TCP、UDP	LDAP
443	TCP	vCenter、vShield Manager、NSX Manager、および ESX の接続
514	UDP	任意。syslog の使用を有効にします。
902	TCP	vCenter および ESX 接続。
903	TCP	vCenter および ESX 接続。
920	TCP、UDP	転送サービスで使用される NFS rpc.statd。
1433	TCP	デフォルトの Microsoft SQL Server データベース ポート。

表 1-7. vCloud Director ホストからの送信パケットを許容する必要があるポート (続き)

ポート	プロトコル	コメント
1521	TCP	デフォルトの Oracle データベース ポート。
5672	TCP、UDP	任意。タスク拡張用 AMQP メッセージ。
61611	TCP	ActiveMQ
61616	TCP	ActiveMQ

- vCloud Director サーバーと vCloud Director データベース サーバー間のトラフィックは、可能であれば専用の非公開ネットワークを介して経路指定してください。
- 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。この間で同じレベル 2 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。

vCloud Director データベースのインストールと構成

vCloud Director セルでは、共有情報の保存にデータベースを使用します。このデータベースは、vCloud Director ソフトウェアのインストールと構成を実行する前に、存在している必要があります。

注意　どのデータベース ソフトウェアを選択した場合でも、使用する vCloud Director に別個に専用のデータベース スキーマを作成する必要があります。vCloud Director では、他の VMware 製品とデータベース スキーマを共有することはできません。

Oracle データベースの構成

Oracle データベースを vCloud Director と一緒に使用する場合、特定の構成要件があります。データベース インスタンスをインストールして構成してから、vCloud Director をインストールする前に vCloud Director データベース ユーザー アカウントを作成します。

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 CPU で構成されたデータベース サーバーであれば、通常の vCloud Director クラスタを適切に使用できます。

2 データベース インスタンスを作成します。

次の形式のコマンドを使用して、単一の CLOUD_DATA テーブルスペースを作成します。

```
Create Tablespace CLOUD_DATA datafile '$ORACLE_HOME/oradata/cloud_data01.dbf' size 1500M autoextend on;
```

3 vCloud Director データベース ユーザー アカウントを作成します。

以下のコマンドは、データベース ユーザー名 **vcloud**、パスワード **vcloudpass** を作成します。

```
Create user $vcloud identified by $vcloudpass default tablespace CLOUD_DATA;
```

注意　vCloud Director データベース ユーザー アカウントを作成するときには、デフォルトのテーブルスペースとして CLOUD_DATA を指定する必要があります。

4 データベース接続、プロセス、およびトランザクションのパラメータを構成します。

各 vCloud Director セルにつき少なくとも 75 個以上の接続、そして Oracle 自身のための使用における約 50 個の接続が可能であるように構成する必要があります。その他の構成パラメータの値は、接続数に基づいて求めることができます。ここでは、<C> は、使用する vCloud Director クラスタ内のセル数を表します。

Oracle 構成パラメータ	<C> セルの値
CONNECTIONS (接続数)	75 * <C> + 50
PROCESSES (プロセス数)	= CONNECTIONS
SESSIONS (セッション数)	= PROCESSES*1.1+5
TRANSACTIONS (トランザクション数)	= SESSIONS*1.1
OPEN_CURSORS	= SESSIONS

5 vCloud Director データベース ユーザー アカウントを作成します。

Oracle システム アカウントを vCloud Director データベース ユーザー アカウントとして使用しないでください。この目的のため、専用のユーザー アカウントを作成する必要があります。以下のシステム権限をアカウントに付与してください。

- CONNECT
- RESOURCE
- CREATE TRIGGER
- CREATE TYPE
- CREATE VIEW
- CREATE MATERIALIZED VIEW
- CREATE PROCEDURE
- CREATE SEQUENCE

6 データベース サービス名は、ネットワークおよびデータベース接続の構成時に使用できるようにメモしておきます。

データベース サービス名を見つけるには、データベース サーバーにあるファイル `$ORACLE_HOME/network/admin/tnsnames.ora` を開き、次の形式のエントリを探します。

```
(SERVICE_NAME = orcl.example.com)
```

Microsoft SQL Server データベースの構成

SQL Server データベースを vCloud Director と併用する場合、特定の構成要件があります。データベース インスタンスをインストールして構成してから、vCloud Director をインストールする前に vCloud Director データベース ユーザー アカウントを作成します。

vCloud Director データベース パフォーマンスは、全体的な vCloud Director パフォーマンスとスケーラビリティの重要な要素です。vCloud Director は、大きな結果セットを保存したり、データを並べ替えたり、同時に読み取り、変更されるデータを管理するときに、SQL Server `tmpdb` ファイルを使用します。このファイルは、vCloud Director が大量の同時負荷を受けた場合、著しく大きくなります。高速の読み書きパフォーマンスを持つ専用ボリュームに `tmpdb` ファイルを作成することをお勧めします。`tmpdb` ファイルと SQL Server パフォーマンスの詳細については、http://msdn.microsoft.com/en-us/library/ms175527.aspx を参照してください。

開始する前に

- Microsoft SQL Server 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。
- Microsoft SQL Server を構成するためには、管理者の認証情報を使用して SQL Server ホスト コンピュータにログオンします。SQL Server を LOCAL_SYSTEM ID、または Windows サービスを実行する権限を持つ任意の ID で実行するように構成できます。

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 CPU で構成されたデータベース サーバーであれば、通常の vCloud Director クラスタを適切に使用できます。

2 SQL Server のセットアップ中に、混在モードの認証を指定してください。

vCloud Director で SQL Server を使用するときに、Windows 認証はサポートされていません。

3 データベース インスタンスを作成します。

以下のスクリプトでは適切な照合順序を指定して、データベースとログ ファイルを作成します。

```
USE [master]
GO
CREATE DATABASE [vcloud] ON PRIMARY
(NAME = N'vcloud', FILENAME = N'C:\vcloud.mdf', SIZE = 100MB, FILEGROWTH = 10% )
LOG ON
(NAME = N'vcdb_log', FILENAME = N'C:\vcloud.ldf', SIZE = 1MB, FILEGROWTH = 10%)
COLLATE Latin1_General_CS_AS
GO
```

SIZE に示されている値は推奨値です。より大きな値を使用することが必要な場合もあります。

4 トランザクション隔離レベルを設定します。

以下のスクリプトでは、データベース隔絶レベルを READ_COMMITTED_SNAPSHOT に設定します。

```
USE [vcloud]
GO
ALTER DATABASE [vcloud] SET SINGLE_USER WITH ROLLBACK IMMEDIATE;
ALTER DATABASE [vcloud] SET ALLOW_SNAPSHOT_ISOLATION ON;
ALTER DATABASE [vcloud] SET READ_COMMITTED_SNAPSHOT ON WITH NO_WAIT;
ALTER DATABASE [vcloud] SET MULTI_USER;
GO
```

トランザクションの隔絶に関する詳細については、http://msdn.microsoft.com/en-us/library/ms173763.aspx を参照してください。

5 vCloud Director データベース ユーザー アカウントを作成します。

以下のスクリプトは、データベース ユーザー名 **vcloud**、パスワード **vcloudpass** を作成します。

```
USE [vcloud]
GO
CREATE LOGIN [vcloud] WITH PASSWORD = 'vcloudpass', DEFAULT_DATABASE =[vcloud],
   DEFAULT_LANGUAGE =[us_english], CHECK_POLICY=OFF
GO
CREATE USER [vcloud] for LOGIN [vcloud]
GO
```

6 vCloud Director データベース ユーザー アカウントに権限を割り当てます。

以下のスクリプトは **db_owner** ロールを 手順 5 で作成されたデータベース ユーザーに割り当てます。

```
USE [vcloud]
GO
sp_addrolemember [db_owner], [vcloud]
GO
```

SSL 証明書の作成

vCloud Director では、クライアントとサーバー間で安全な通信を行うために SSL を使用します。vCloud Director サーバー グループをインストールして構成する前に、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。

vCloud Director サーバーごとに、2 つの異なる SSL エンドポイントをサポートできるように 2 つの IP アドレスが必要です。各エンドポイントには独自の SSL 証明書が必要です。どちらのエンドポイントの証明書も X.500 の識別名を含む必要があります。多くの認証局では、認証局が許可する証明書に X.509 のサブジェクト別名拡張子を含めることを推奨しています。vCloud Director では証明書にサブジェクト別名を含める必要はありません。

手順

1 このサーバーの IP アドレスを一覧表示します。

このサーバーの 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。

2 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を取得します。

```
nslookup <ip-address>
```

3 各 IP アドレスとそれに関連付けられた完全修飾ドメイン名、および vCloud Director でアドレスを HTTP サービスとコンソール プロキシ サービスのどちらに使用するかをメモしておきます。

証明書の作成時には完全修飾ドメイン名が、ネットワークおよびデータベース接続の構成時には IP アドレスが必要になります。IP アドレスが他の完全修飾ドメイン名によってアクセス可能な場合、証明書にサブジェクト別名を含めるときにそれらのドメイン名と IP アドレスも必要になるため、メモしておきます。

4 証明書を作成します。

信頼できる認証局で署名された証明書か、自己署名付き証明書を使用できます。

注意　署名付き証明書は、最高レベルの信頼を提供します。

署名付き SSL 証明書の作成とインポート

署名付き証明書は、SSL 通信に最高レベルの信頼を提供します。

各 vCloud Director サーバーを使用するには、Java キーストア ファイル内に 2 つの SSL 証明書が必要です。1 つは HTTP サービス用で、もう 1 つはコンソール プロキシ サービス用です。信頼できる認証局で署名された証明書か、自己署名付き証明書を使用できます。署名付き証明書は、最高レベルの信頼を提供します。

重要　これらの例では 2,048 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、1,024 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。

自己署名付き証明書を作成してインポートするには、「自己署名付き SSL 証明書の作成 (P. 21)」を参照してください。

開始する前に

- このサーバー上の完全修飾ドメイン名および関連付けられた IP アドレスのリストを生成します。
- HTTP サービスに使用するアドレス、およびコンソール プロキシ サービスに使用するアドレスを選択します。「SSL 証明書の作成 (P. 18)」 を参照してください。
- **keytool** コマンドを使用して証明書を作成できるように、Java バージョン 7 ランタイム環境のあるコンピュータにアクセスできることを確認します。vCloud Director インストーラでは **keytool** のコピーが **/opt/vmware/vcloud-director/jre/bin/keytool** に置かれますが、この手順は Java バージョン 7 ランタイム環境がインストールされていればどのコンピュータでも実行できます。**keytool** で他のソースから作成され

た証明書を vCloud Director に使用することはできません。vCloud Director ソフトウェアをインストールして構成する前に証明書を作成してインポートしておくと、インストールと構成のプロセスが簡素化されます。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。これらの例では、キーストアのパスワードは <passwd> として表されています。

- どちらのエンドポイントの証明書も X.500 の識別名を含む必要があります。多くの認証局では、認証局が許可する証明書に X.509 のサブジェクト別名拡張子を含めることを推奨しています。vCloud Director では証明書にサブジェクト別名を含める必要はありません。 **–dname** および**–ext** オプションを含む **keytool** コマンドについて理解してください。
- keytool の **–dname** オプションの引数に必要な情報を収集します。

表 1-8. keytool の –dname オプションに必要な情報

X.500 識別名のサブパート	keytool のキーワード	説明	例
commonName	CN	このエンドポイントの IP アドレスに関連付けられた完全修飾ドメイン名。	CN=vcd1.example.com
organizationalUnit	OU	この証明書が関連付けられた組織内の、部署または課などの組織単位の名前	OU=Engineering
organizationName	O	この証明書が関連付けられた組織の名前	O=Example Corporation
localityName	L	組織が存在する市区町村の名前。	L=Palo Alto
stateName	S	組織が存在する都道府県または州の名前。	S=California
country	C	組織が存在する国の名前。	C=US

手順

1 HTTP サービスについて信頼できない証明書を作成します。

この例のコマンドでは、**certificates.ks** という名前のキーストア ファイルに信頼できない証明書が作成されます。わかりやすくするために、**keytool** オプションは別の行に配置されています。**–dname** オプションの引数に指定された X.500 識別名情報では、「前提条件」に示された値を使用します。 **–ext** オプションの引数に示された DNS および IP 値は標準の値です。**–dname** オプション引数の **commonName** (CN) 値に指定されたものを含めて、このエンドポイントが到達できるすべての DNS 名を含めてください。ここに示された IP アドレスも含めることができます。

```
keytool
   –keystore certificates.ks
   –alias http
   –storepass <passwd>
   –keypass <passwd>
   –storetype JCEKS
   –genkeypair
   –keyalg RSA
   –keysize 2048
   –validity 365
   –dname "CN=vcd1.example.com, OU=Engineering, O=Example Corp, L=Palo Alto
S=California C=US"
   –ext "san=dns:vcd1.example.com,dns:vcd1,ip:10.100.101.9"
```

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

2 コンソール プロキシ サービスについて信頼できない証明書を作成します。

このコマンドでは、手順 1 で作成したキーストア ファイルに信頼できない証明書を追加します。わかりやすくするために、keytool オプションは別の行に配置されています。–dname オプションの引数に指定された X.500 識別名情報では、「前提条件」に示された値を使用します。 –ext オプションの引数に示された DNS および IP 値は標準の値です。–dname オプション引数の commonName (CN) 値に指定されたものを含めて、このエンドポイントが到達できるすべての DNS 名を含めてください。ここに示された IP アドレスも含めることができます。

```
keytool
   –keystore certificates.ks
   –alias consoleproxy
   –storepass <passwd>
   –keypass <passwd>
   –storetype JCEKS
   –genkeypair
   –keyalg RSA
   –keysize 2048
   –validity 365
   –dname "CN=vcd2.example.com, OU=Engineering, O=Example Corp, L=Palo Alto
S=California C=US"
   –ext "san=dns:vcd2.example.com,dns:vcd2,ip:10.100.101.10"
```

3 HTTP サービスへの証明書署名要求を作成します。

このコマンドでは、証明書署名要求をファイル http.csr 内に作成します。

```
keytool –keystore certificates.ks –storetype JCEKS –storepass <passwd> –certreq –
alias http –file http.csr
```

4 コンソール プロキシ サービスについて、証明書署名要求を作成します。

このコマンドでは、証明書署名要求をファイル consoleproxy.csr 内に作成します。

```
keytool –keystore certificates.ks –storetype JCEKS –storepass <passwd> –certreq –
alias consoleproxy –file consoleproxy.csr
```

5 証明書署名要求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。

6 署名付き証明書を受信したら、キーストア ファイルにインポートします。

a 認証局のルート証明書をキーストア ファイルにインポートします。

このコマンドでは、ルート証明書を root.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 –storetype JCEKS –storepass <passwd> –keystore certificates.ks –import
–alias root –file root.cer
```

b (オプション) 中間証明書を受信したら、キーストア ファイルにインポートします。

このコマンドでは、中間証明書を 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 –storetype JCEKS –storepass <passwd> –keystore certificates.ks –import
–alias intermediate –file intermediate.cer
```

c HTTP サービスの証明書をインポートします。

このコマンドでは、証明書を **http.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 –storetype JCEKS –storepass <passwd> –keystore certificates.ks –import
–alias http –file http.cer
```

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。

このコマンドでは、証明書を **consoleproxy.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 –storetype JCEKS –storepass <passwd> –keystore certificates.ks –import
–alias consoleproxy –file consoleproxy.cer
```

7 すべての証明書がインポートされたことを確認するには、キーストア ファイルの内容を一覧表示します。

```
keytool –storetype JCEKS –storepass <passwd> –keystore certificates.ks –list
```

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

次に進む前に

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。「ネットワークおよびデータベース接続の構成 (P. 30)」を参照してください。

自己署名付き SSL 証明書の作成

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

各 vCloud Director サーバーを使用するには、Java キーストア ファイル内に 2 つの SSL 証明書が必要です。1 つは HTTP サービス用で、もう 1 つはコンソール プロキシ サービス用です。信頼できる認証局で署名された証明書か、自己署名付き証明書を使用できます。署名付き証明書は、最高レベルの信頼を提供します。

重要 これらの例では 2,048 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、1,024 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。

署名付き証明書を作成してインポートするには、「署名付き SSL 証明書の作成とインポート (P. 18)」を参照してください。

開始する前に

- このサーバー上の完全修飾ドメイン名および関連付けられた IP アドレスのリストを生成します。
- HTTP サービスに使用するアドレス、およびコンソール プロキシ サービスに使用するアドレスを選択します。「SSL 証明書の作成 (P. 18)」 を参照してください。
- **keytool** コマンドを使用して証明書を作成できるように、Java バージョン 7 ランタイム環境のあるコンピュータにアクセスできることを確認します。vCloud Director インストーラでは **keytool** のコピーが **/opt/vmware/vcloud-director/jre/bin/keytool** に置かれますが、この手順は Java バージョン 7 ランタイム環境がインストールされていればどのコンピュータでも実行できます。**keytool** で他のソースから作成された証明書を vCloud Director に使用することはできません。vCloud Director ソフトウェアをインストールして構成する前に証明書を作成してインポートしておくと、インストールと構成のプロセスが簡素化されます。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。これらの例では、キーストアのパスワードは <passwd> として表されています。

- どちらのエンドポイントの証明書も X.500 の識別名を含む必要があります。多くの認証局では、認証局が許可する証明書に X.509 のサブジェクト別名拡張子を含めることを推奨しています。vCloud Director では証明書にサブジェクト別名を含める必要はありません。 **–dname** および**–ext** オプションを含む **keytool** コマンドについて理解してください。
- keytool の **–dname** オプションの引数に必要な情報を収集します。

表 1-9. keytool の **–dname** オプションに必要な情報

X.500 識別名のサブパート	keytool のキーワード	説明	例
commonName	CN	このエンドポイントの IP アドレスに関連付けられた完全修飾ドメイン名。	CN=vcd1.example.com
organizationalUnit	OU	この証明書が関連付けられた組織内の、部署または課などの組織単位の名前	OU=Engineering
organizationName	O	この証明書が関連付けられた組織の名前	O=Example Corporation
localityName	L	組織が存在する市区町村の名前。	L=Palo Alto
stateName	S	組織が存在する都道府県または州の名前。	S=California
country	C	組織が存在する国の名前。	C=US

手順

1 HTTP サービスについて信頼できない証明書を作成します。

この例のコマンドでは、**certificates.ks** という名前のキーストア ファイルに信頼できない証明書が作成されます。わかりやすくするために、**keytool** オプションは別の行に配置されています。**–dname** オプションの引数に指定された X.500 識別名情報では、「前提条件」に示された値を使用します。 **–ext** オプションの引数に示された DNS および IP 値は標準の値です。**–dname** オプション引数の **commonName** (CN) 値に指定されたものを含めて、このエンドポイントが到達できるすべての DNS 名を含めてください。ここに示された IP アドレスも含めることができます。

```
keytool
   –keystore certificates.ks
   –alias http
   –storepass <passwd>
   –keypass <passwd>
   –storetype JCEKS
   –genkeypair
   –keyalg RSA
   –keysize 2048
   –validity 365
   –dname "CN=vcd1.example.com, OU=Engineering, O=Example Corp, L=Palo Alto
S=California C=US"
   –ext "san=dns:vcd1.example.com,dns:vcd1,ip:10.100.101.9"
```

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

2 コンソール プロキシ サービスについて信頼できない証明書を作成します。

このコマンドでは、手順 1 で作成したキーストア ファイルに信頼できない証明書を追加します。わかりやすくするために、**keytool** オプションは別の行に配置されています。**–dname** オプションの引数に指定された X.500 識別名情報では、「前提条件」に示された値を使用します。 **–ext** オプションの引数に示された DNS および IP 値は標準の値です。**–dname** オプション引数の **commonName** (CN) 値に指定されたものを含めて、このエンドポイントが到達できるすべての DNS 名を含めてください。ここに示された IP アドレスも含めることができます。

```
keytool
   –keystore certificates.ks
   –alias consoleproxy
   –storepass <passwd>
   –keypass <passwd>
   –storetype JCEKS
   –genkeypair
   –keyalg RSA
   –keysize 2048
   –validity 365
   –dname "CN=vcd2.example.com, OU=Engineering, O=Example Corp, L=Palo Alto
S=California C=US"
   –ext "san=dns:vcd2.example.com,dns:vcd2,ip:10.100.101.10"
```

3 すべての証明書がインポートされたことを確認するには、キーストア ファイルの内容を一覧表示します。

```
keytool –storetype JCEKS –storepass <passwd> –keystore certificates.ks –list
```

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

次に進む前に

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。「ネットワークおよびデータベース接続の構成 (P. 30)」を参照してください。

新しい vCloud Director をインストールするための vShield Manager のインストールおよび構成

vCloud Director は vShield Manager または NSX Manager のいずれかがある場合に、クラウドにネットワーク サービスを提供します。vCloud Director の新規インストールを実行する前に、vShield Manager または NSX Manager のいずれかをインストールおよび構成して、vShield Manager または NSX Manager の一意のインスタンスに、vCloud Director インストールに含める予定の各 vCenter Server を関連付ける必要があります。

vShield Manager は、VMware vCloud Networking and Security ダウンロードに含まれています。vCloud Director と互換性のある vShield Manager のサポート対象バージョンの最新情報については、VMware Partner Centra にある「VMware 製品の互換性マトリックス」を参照してください。VMware パートナー アカウント情報を使用して VMware Partner Central にログインします。ネットワーク要件の詳細については、「vCloud Director のハードウェアおよびソフトウェア要件 (P. 9)」を参照してください。

重要　この手順は、vCloud Director の新規インストールを実行している場合のみ適用されます。vCloud Director の既存インストールをアップグレードしている場合は、第 3 章「vCloud Director のアップグレード (P. 39)」を参照してください。

開始する前に

- vCenter Server システムがそれぞれ vShield 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。

- 『vShield インストールおよびアップグレード ガイド』に記載された vShield 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。

手順

1 インストールした vShield 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。

2 インストールした vShield Manager 仮想アプライアンスを、計画した vCloud Director インストールで vCloud Director に追加する予定の vCenter Server システムに関連付けます。

次に進む前に

関連付けられた vShield Manager 内で VXLAN サポートを構成します。vCloud Director が VXLAN ネットワーク プールを作成し、プロバイダ VDC にネットワーク リソースを提供します。関連付けられた vShield 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 サポートの構成方法の詳細については、『vShield 管理ガイド』を参照してください。

新しい vCloud Director をインストールするための NSX Manager のインストールおよび構成

vCloud Director は vShield Manager または NSX Manager のいずれかがある場合に、クラウドにネットワーク サービスを提供します。vCloud Director の新規インストールを実行する前に、vShield Manager または NSX Manager のいずれかをインストールおよび構成して、vShield Manager または NSX Manager の一意のインスタンスに、vCloud Director インストールに含める予定の各 vCenter Server を関連付ける必要があります。

NSX は VMware NSX for vSphere のダウンロードに含まれています。 vCloud Director と互換性のある NSX Manager のサポート対象バージョンの最新情報については、VMware Partner Central にある「VMware 製品の相互運用性マトリクス」を参照してください。VMware パートナー アカウント情報を使用して VMware Partner Central にログインします。 ネットワーク要件の詳細については、「vCloud Director のハードウェアおよびソフトウェア要件 (P. 9)」を参照してください。

重要　この手順は、vCloud Director の新規インストールを実行している場合のみ適用されます。vCloud Director の既存インストールをアップグレードしている場合は、第 3 章「vCloud Director のアップグレード (P. 39)」を参照してください。

開始する前に

- vCenter Server システムがそれぞれ 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。
- 『NSX インストールおよびアップグレード ガイド』に記載された 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。

手順

1 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。

2 インストールした NSX Manager 仮想アプライアンスを、計画した vCloud Director のインストールで vCloud Director に追加する予定の vCenter Server システムに関連付けます。

次に進む前に

関連付けられた NSX Manager 内で VXLAN サポートを構成します。vCloud Director が VXLAN ネットワーク プールを作成し、プロバイダ VDC にネットワーク リソースを提供します。関連付けられた NSX Manager で VXLAN サポートが構成されていない場合は、プロバイダ VDC にネットワーク プール エラーが表示され、ユーザーが別のタイプのネットワーク プールを作成し、それをプロバイダ VDC に関連付ける必要があります。VXLAN サポートの構成の詳細については、『NSX 管理ガイド』を参照してください。

AMQP ブローカーのインストールと構成

AMQP (Advanced Message Queuing Protocol) はエンタープライズ システムの柔軟なメッセージングをサポートするメッセージ キューのオープン スタンダードです。vCloud Director は、RabbitMQ などの AMQP ブローカーと連携するように構成できる AMQP サービスを含みます。このサービスを使用してクラウドのイベントに関する通知のストリームをクラウドのオペレータに提供できます。このサービスを使用する場合、AMQP ブローカーをインストールし、構成する必要があります。

vCloud Director での AMQP ブローカーの使用はオプションですが、多くの統合では vCloud Director との通信に AMQP が使用されます。使用する予定の統合については、インストールと構成のマニュアルを参照してください。

手順

1 http://info.vmware.com/content/12834_rabbitmq から RabbitMQ Server をダウンロードします。

2 RabbitMQ インストールの手順に従って、RabbitMQ を任意のホストにインストールします。

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

3 RabbitMQ インストール中に、この RabbitMQ インストールと連携するように vCloud Director を構成するときに指定する必要がある値を書き留めておきます。

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

次に進む前に

デフォルトでは、vCloud Director AMQP サービスは暗号化されていないメッセージを送信します。SSL を使用してこれらのメッセージを暗号化するために構成する場合、vCloud Director サーバーで Java ランタイム環境のデフォルト JCEKS トラスト ストアを使用することで、ブローカーの証明書を検証します。Java ランタイム環境は、一般的に `$JRE_HOME/lib/security/cacerts` ディレクトリにあります。

vCloud Director AMQP サービスで SSL を使用するには、vCloud Director Web コンソールの [拡張性] ページにある [AMQP ブローカーの設定] セクションで [SSL を使用] を選択し、次のいずれかを指定します。

- SSL 証明書のパス名
- JCEKS 信頼ストアのパス名とパスワード

AMQP ブローカーの証明書の有効性を確認する必要がない場合は、[すべての証明書を承認] を選択できます。

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

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

手順

1 VMware パッケージ パブリック キーを保存するためにディレクトリを作成します。

2 Web ブラウザを使用して http://packages.vmware.com/tools/keys ディレクトリからすべての VMware パブリック パッケージ パブリック キーをダウンロードします。

3 作成したディレクトリにキー ファイルを保存します。

4 ダウンロードする各キーに対して、以下のコマンドを実行してキーをインポートします。

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

<key_path> はキーを保存するディレクトリです。

<key_name> は、キーのファイル名です。

vCloud Director Server グループの作成 2

vCloud Director サーバー グループは、共通のデータベースおよび他の構成の詳細を共有する 1 つ以上の vCloud Director サーバーで構成されます。サーバー グループを作成するには、グループの最初のメンバーに vCloud Director ソフトウェアをインストールして、構成します。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。

vCloud Director Server グループ作成の前提条件

重要　この手順は、新しいインストールのみを対象としています。既存の vCloud Director インストールをアップグレードしている場合は、第 3 章「vCloud Director のアップグレード (P. 39)」 を参照してください。

vCloud Director のインストールと構成を開始する前に、次のタスクをすべて完了します。

1 サポート対象の vCenter Server システムが実行されていて、vCloud Director で使用できるように適切に構成されていることを確認します。サポート対象バージョンと構成要件については、「サポート対象プラットフォーム (P. 9)」を参照してください。

2 サポート対象の vShield Manager または NSX Manager が実行されていること、vCenter Server システムに関連付けられていること、および vCloud Director で使用できるよう適切に構成されていることを確認します。サポート対象バージョンについては、「サポート対象プラットフォーム (P. 9)」を参照してください。インストールと構成の詳細については、「新しい vCloud Director をインストールするための vShield Manager のインストールおよび構成 (P. 23)」 および 「新しい vCloud Director をインストールするための NSX Manager のインストールおよび構成 (P. 24)」 を参照してください。

3 vCloud Director ソフトウェアを実行できるようサポートされているサーバー プラットフォームが 1 つ以上あり、そのサーバー プラットフォームに適切なサイズのメモリおよびストレージが構成されていることを確認します。サポート対象プラットフォームと構成要件については、「サポート対象の vCloud Director サーバー オペレーティング システム (P. 10)」を参照してください。

   - サーバー グループの各メンバーは、以下の 2 つの IP アドレスを必要とします。1 つは HTTP サービスの SSL 接続をサポートし、もう 1 つはコンソール プロキシ サービスの接続をサポートします。
   - 各サーバーには IP アドレスごとに SSL 証明書が必要です。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。「SSL 証明書の作成 (P. 18)」 を参照してください。
   - 転送サービスの場合、各サーバーは NFS またはその他の共有ストレージ ボリュームを `/opt/vmware/vcloud-director/data/transfer` にマウントする必要があります。このボリュームにはサーバ グループのすべてのメンバーがアクセスできる必要があります。「vCloud Director のネットワーク構成要件の要約 (P. 13)」 を参照してください。
   - 各サーバーには、Microsoft Sysprep デプロイ パッケージへのアクセス権が必要です。「Microsoft Sysprep ファイルのサーバーへのインストール (P. 35)」 を参照してください。

4 vCloud Director データベースを作成し、グループのすべてのサーバーにアクセス可能であることを確認します。サポート対象データベース ソフトウェアの一覧については、「サポート対象の vCloud Director データベース (P. 10)」を参照してください。

   - vCloud Director データベース ユーザーのデータベース アカウントを作成したことと、そのアカウントに必要なデータベース権限がすべて付与されていることを確認します。「vCloud Director データベースのインストールと構成 (P. 15)」 を参照してください。
   - データベース サーバーが再起動されるとデータベース サービスが開始することを確認します。

5 すべての vCloud Director サーバー、データベース サーバー、すべての vCenter Server システム、およびこれらの vCenter Server システムに関連付けられた vShield Manager または NSX Manager コンポーネントが、「vCloud Director のネットワーク構成要件の要約 (P. 13)」 に記載されているように、それぞれの名前を相互に解決できることを確認します。

6 すべての vCloud Director サーバーとデータベース サーバーが、「vCloud Director のネットワーク構成要件の要約 (P. 13)」にある許容値の範囲内でネットワーク タイム サーバーと同期していることを確認します。

7 ユーザーまたはグループを LDAP サービスからインポートする予定がある場合、サービスが各 vCloud Director サーバーにアクセスできることを確認します。

8 「ネットワーク セキュリティ要件 (P. 14)」に示されているように、ファイアウォール ポートを開きます。vCloud Director システムと vCenter Server システムの間でポート 443 が開いている必要があります。

この章では次のトピックについて説明します。

サーバー グループの最初のメンバーに対する vCloud Director ソフトウェアのインストールと構成

vCloud Director のすべてのメンバーは、グループの最初のメンバーをインストールおよび構成するときに指定するデータベース接続と他の構成の詳細を共有します。これらの詳細は、グループにメンバーを追加するときに使用する必要がある応答ファイルでキャプチャされます。

vCloud Director ソフトウェアは、`vmware-vcloud-director-8.0.0-nnnnnn.bin` という名前のデジタル署名された Linux 実行可能ファイルとして配布されます。nnnnnn はビルド番号を示します。

vCloud Director インストーラでは、ターゲット サーバーがプラットフォームのすべての前提条件を満たしていることを確認し、vCloud Director ソフトウェアをターゲット サーバーにインストールします。ターゲット サーバーにソフトウェアをインストールしたら、サーバーのネットワークおよびデータベース接続を構成するスクリプトを実行する必要があります。このスクリプトは、このサーバー 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。

開始する前に

- ターゲット サーバーとそこに接続するネットワークが、「vCloud Director のネットワーク構成要件の要約 (P. 13)」で指定した要件を満たしていることを確認します。
- ターゲット サーバー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。
- ターゲット サーバーが `/opt/vmware/vcloud-director/data/transfer` に共有転送サービス ストレージ ボリュームをマウントしてい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には、ターゲット サーバーに 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 (P. 25)」 を参照してください。

手順

1 ターゲット サーバーにルート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。

CD またはその他のメディアでソフトウェアを購入した場合、インストール ファイルをすべてのターゲット サーバーからアクセスできる場所にコピーします。

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

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

```
[root@cell1 /tmp]# md5sum <installation-file>
<checksum-value> <installation-file>
```

このコマンドで生成される <checksum-value> と、ダウンロードページからコピーした MD5 チェックサムを比較します。

4 インストール ファイルが実行可能であることを確認します。

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

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

5 コンソール、シェル、またはターミナル ウィンドウで、インストール ファイルを実行します。

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

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

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

注意　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、ターゲット サーバーに VMware パブリック キーをインストールしなかった場合は、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
```

インストーラが動作すると、これらのアクションが実行されます。

a　ホストがすべての要件を満たすことを確認する

b　インストール ファイルのデジタル署名を検証する

c　**vcloud** ユーザーとグループを作成する

d　vCloud Director RPM パッケージを展開する

e　ソフトウェアをインストールする

ソフトウェアがインストールされると、インストーラにより、構成スクリプトを実行してサーバーの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。

次に進む前に

構成スクリプトを実行するかどうかを決定します。

- 「vCloud Director Server グループ作成の前提条件 (P. 27)」 に示される前提条件を満たしたら、構成スクリプトを実行できます。**y** を入力して Enter を押します。
- 構成スクリプトを実行する準備ができていない場合は、**n** を入力して Enter を押し、シェルに戻ります。

構成スクリプトの実行に関する詳細については、「ネットワークおよびデータベース接続の構成 (P. 30)」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

サーバーに vCloud Director ソフトウェアをインストールすると、インストーラから、サーバーのネットワーク接続とデータベース接続を構成するためのスクリプトを実行するよう要求するメッセージが表示されます。

構成スクリプトを実行する前に、サーバーに vCloud Director ソフトウェアをインストールする必要があります。インストールが完了するとインストーラからスクリプトを実行するようにメッセージが表示されますが、スクリプトは後で実行することもできます。

vCloud Director ソフトウェアをインストールした後でスクリプトを実行するには、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。

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

構成スクリプトでは、1 つの vCloud Director サーバーに対してネットワークおよびデータベース接続を作成します。スクリプトではまた、以降のサーバー インストールで使用できるようにデータベース接続情報を保存した応答ファイルも作成されます。

注意　構成スクリプトを実行してサーバー グループの最初のメンバーを構成した後で、グループに追加メンバーを構成する場合は、**-r** オプションを使用し、応答ファイルのパス名を指定する必要があります。「応答ファイルの保護と再利用 (P. 33)」 を参照してください。

開始する前に

- サポートされているタイプのデータベースに vCloud Director サーバーからアクセスできることを確認します。「vCloud Director データベースのインストールと構成 (P. 15)」 および 「vCloud Director のハードウェアおよびソフトウェア要件 (P. 9)」 を参照してください。
- 次の情報を使用できることを確認します。
  - このサーバーの SSL 証明書が含まれるキーストア ファイルの場所とパスワード。「署名付き SSL 証明書の作成とインポート (P. 18)」 を参照してください。構成スクリプトの実行は特権 ID のみに制限されないため、キーストア ファイルとそのディレクトリはすべてのユーザーから読み取り可能である必要があります。
  - 各 SSL 証明書のパスワード。
  - データベース サーバーのホスト名または IP アドレス。
  - データベース名と接続ポート。
  - データベース ユーザーの認証情報 (ユーザー名とパスワード)。このユーザーには、特定のデータベース権限が必要です。「vCloud Director データベースのインストールと構成 (P. 15)」 を参照してください。

手順

1 このホスト上で実行される HTTP サービスとコンソール プロキシ サービスに使用する IP アドレスを指定します。

サーバー グループの各メンバーは、2 つの異なる SSL 接続をサポートできるように 2 つの IP アドレスが必要です。1 つは HTTP サービス用で、もう 1 つはコンソール プロキシ サービス用です。構成プロセスを開始するには、スクリプトで検出された IP アドレスのうちのどれを各サービスに使用するかを選択します。

```
Please indicate which IP address available on this machine should be used for the
HTTP service and which IP address should be used for the remote console proxy. The
HTTP service IP address is used for accessing the user interface and the REST
API.The remote console proxy IP address is used for all remote console (VMRC)
connections and traffic. Please enter your choice for the HTTP service IP address:
1: 10.17.118.158 2: 10.17.118.159 Choice [default=1]:2
                        Please enter your choice for the remote console proxy IP
address 1: 10.17.118.158 Choice [default=1]:
```

2 Java キーストア ファイルへのフル パスを指定します。

```
Please enter the path to the Java keystore containing your SSL certificates and
private keys:/opt/keystore/certificates.ks
```

3 キーストアと証明書のパスワードを入力します。

```
Please enter the password for the keystore: Please enter the private key password
for the 'http' SSL certificate: Please enter the private key password for the
'consoleproxy' SSL certificate:
```

4 監査メッセージ処理オプションを構成します。

各 vCloud Director セル内のサービスは、監査メッセージを vCloud Director データベースにログとして記録し、メッセージは 90 日間保存されます。監査メッセージの保存期間を長くするには、監査メッセージを vCloud Director データベースだけでなく `syslog` ユーティリティに送信するように vCloud Director サービスを構成できます。

オプション	操作
監査メッセージを `syslog` と vCloud Director データベースの両方にログとして記録する場合は、	`syslog` のホスト名または IP アドレスを入力します。
監査メッセージを vCloud Director データベースにのみログとして記録する場合は、	Enter を押します。

```
If you would like to enable remote audit logging to a syslog host please enter the
hostname or IP address of the syslog server. Audit logs are stored by vCloud
Director for 90 days. Exporting logs via syslog will enable you to preserve them
for as long as necessary. Syslog host name or IP address [press Enter to skip]:
10.150.10.10
```

5 `syslog` プロセスが指定したサーバーを監視するポートを指定します。

デフォルトはポート 514 です。

```
What UDP port is the remote syslog server listening on? The standard syslog port is
514. [default=514]: Using default value "514" for syslog port.
```

6 データベース タイプを指定するか、Enter を押してデフォルト値を受け入れます。

```
The following database types are supported: 1. Oracle 2. Microsoft SQL Server Enter
the database type [default=1]: Using default value "1" for database type.
```

7 データベース接続情報を指定します。

スクリプトに必要な情報は、選択したデータベース タイプに応じて異なります。この例では、Oracle データベースを指定した後に表示されるプロンプトを示しています。他のデータベース タイプで表示されるプロンプトもほぼ同じです。

a データベース サーバーのホスト名または IP アドレス を入力します。

```
Enter the host (or IP address) for the database:10.150.10.78
```

b データベース ポートを入力するか、Enter を押してデフォルト値を受け入れます。

```
Enter the database port [default=1521]: Using default value "1521" for port.
```

c データベース サービス名を入力します。

```
Enter the database service name [default=oracle]:orcl.example.com
```

Enter を押すと、構成スクリプトでデフォルト値が使用されますが、インストール環境によってはデフォルト値が適切でない場合もあります。Oracle データベースのデータベース サービス名を見つける方法については、「Oracle データベースの構成 (P. 15)」を参照してください。

d データベース ユーザー名とパスワードを入力します。

```
Enter the database username:vcloud
                                    Enter the database password:
```

このスクリプトは、指定した情報を検証した後、引き続き 3 つのステップを実行します。

1 データベースを初期化し、このサーバーをデータベースに接続します。

2 このホスト上で vCloud Director サービスを開始できます。

3 vCloud Director サービスの開始後、セットアップ ウィザードに接続するための URL を表示します。

このフラグメントは、スクリプトの通常の完了プロセスを示しています。

```
Connecting to the database: jdbc:oracle:thin:vcloud/vcloud@10.150.10.78:1521/vcloud
                ...........
                Database configuration complete. Once the vCloud Director server has
been started you will be able to access the first-time setup wizard at this URL:
http://vcloud.example.com Would you like to start the vCloud Director service now? If
you choose not to start it now, you can manually start it at any time using this
command: service vmware-vcd start
                Start it now? [y/n]:y
                Starting the vCloud Director service (this may take a moment). The
service was started; it may be several minutes before it is ready for use.Please check
the logs for complete details.vCloud Director configuration is now complete.Exiting...
```

次に進む前に

注意 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応答は、このサーバーの **/opt/vmware/vcloud-director/etc/responses.properties** にあるファイルに保存されます。このファイルには、サーバー グループにサーバー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。

このグループにサーバーを追加するには、「サーバー グループの追加メンバーに対する vCloud Director ソフトウェアのインストール (P. 33)」を参照してください。

すべてのサーバーで vCloud Director サービスが実行中になったら、スクリプト完了時に表示された URL でセットアップ ウィザードを開くことができます。第 4 章「vCloud Director セットアップ (P. 51)」 を参照してください。

応答ファイルの保護と再利用

最初に vCloud Director サーバーを構成したときに指定したネットワークおよびデータベース接続の詳細が、応答ファイルに保存されます。このファイルには、サーバー グループにサーバー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。

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

手順

1 応答ファイルを保護します。

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。

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

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

インストーラにより、このユーザーとグループが作成されます。

---

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

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

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

次に進む前に

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。

サーバー グループの追加メンバーに対する vCloud Director ソフトウェアのインストール

vCloud Director サーバー グループにはいつでもサーバーを追加できます。サーバー グループのすべてのサーバーは、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、追加メンバーを構成する場合は、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して、この情報を指定する必要があります。

開始する前に

- このサーバー グループに最初のメンバーをインストールおよび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。「応答ファイルの保護と再利用 (P. 33)」 を参照してください。
- このサーバーから vCloud Director データベースにアクセスできることを確認します。

- このサーバーに対して作成した SSL 証明書がインストーラがアクセスできる場所にインストールされていることを確認します。「署名付き SSL 証明書の作成とインポート (P. 18)」 を参照してください。構成スクリプトの実行は特権 ID のみに制限されないため、キーストア ファイルとそのパスはすべてのユーザーから読み取り可能である必要があります。サーバー グループのすべてのメンバーに同じキーストア パス (`/tmp/certificates.ks` など) 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。
- 次の情報を使用できることを確認します。
  - このサーバーの SSL 証明書が含まれるキーストア ファイルのパスワード。
  - 各 SSL 証明書のパスワード。

手順

1 ターゲット サーバーにルート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。

CD またはその他のメディアでソフトウェアを購入した場合、インストール ファイルをすべてのターゲット サーバーからアクセスできる場所にコピーします。

3 インストール ファイルが実行可能であることを確認します。

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

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

4 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。

5 コンソール、シェル、またはターミナル ウィンドウで、`-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、インストール ファイルを実行します。

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

```
[root@cell1 /tmp]#
                        ./<installation-file> -r /<path-to-response-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。

注意　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、ターゲット サーバーに VMware パブリック キーをインストールしなかった場合は、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
```

インストーラが`-r` オプションを実行すると、これらのアクションが実行されます。

a　ホストがすべての要件を満たすことを確認する

b　インストール ファイルのデジタル署名を検証する

c　`vcloud` ユーザーとグループを作成する

d　vCloud Director RPM パッケージを展開する

e　ソフトウェアをインストールする

f　vcloud.vcloud から読み取りできる場所に応答ファイルをコピーする

g 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する

構成スクリプトを実行すると、応答ファイルに保存されたパスで証明書 (`/tmp/certificates.ks` など) が検索され、キーストアと証明書のパスワードを指定するプロンプトが表示されます。応答ファイルに保存されたパス名で有効な証明書が検出されない場合は、証明書のパス名を入力するように指示するプロンプトが表示されます。

6 (オプション) このサーバー グループに他のサーバーを追加するには、上記の手順を繰り返します。

次に進む前に

一部の古い Microsoft オペレーティング システムに対してゲストのカスタマイズをクラウドでサポートする必要がある場合は、サーバー グループのすべてのメンバーに Sysprep ファイルをインストールします。「Microsoft Sysprep ファイルのサーバーへのインストール (P. 35)」 を参照してください。

構成スクリプトが終了し、すべてのサーバーで vCloud Director サービスが実行中になったら、スクリプト完了時に表示された URL でセットアップ ウィザードを開くことができます。第 4 章「vCloud Director セットアップ (P. 51)」 を参照してください。

Microsoft Sysprep ファイルのサーバーへのインストール

vCloud Director が特定の古い Windows ゲスト OS を使用した仮想マシン上でゲストのカスタマイズを実行するには、サーバー グループのメンバーごとに適切な Microsoft Sysprep ファイルをインストールしておく必要があります。

Sysprep ファイルは、一部の古い Microsoft オペレーティング システムにのみ必要です。クラウドでこれらのオペレーティング システムのゲストのカスタマイズをサポートする必要がない場合は、Sysprep ファイルのインストールは不要です。

Sysprep バイナリ ファイルをインストールするには、それらをサーバー上の特定の場所にコピーします。サーバー グループの各メンバーに対してファイルをコピーする必要があります。

開始する前に

Windows 2003 および Windows XP の 32 ビットおよび 64 ビットの Sysprep バイナリ ファイルにアクセスできることを確認します。

手順

1 ターゲット サーバーにルートとしてログインします。

2 ディレクトリを `$VCLOUD_HOME/guestcustomization/default/windows` に変更します。

```
[root@cell1 /]# cd /opt/vmware/vcloud-director/guestcustomization/default/windows
```

3 `sysprep` という名前のディレクトリを作成します。

```
[root@cell1 /opt/vmware/vcloud-director/guestcustomization/default/windows]#
mkdir sysprep
```

4 Sysprep バイナリ ファイルを必要とする各ゲスト OS に対して、`$VCLOUD_HOME/guestcustomization/default/windows/sysprep` のサブディレクトリを作成します。

サブディレクトリ名は、ゲスト OS に特有のものとなります。

表 2-1. Sysprep ファイルのサブディレクトリの割り当て

ゲスト OS	$VCLOUD_HOME/guestcustomization/default/windows/sysprep の下に作成するサブディレクトリ
Windows 2003 (32 ビット)	svr2003
Windows 2003 (64 ビット)	svr2003-64
Windows XP (32 ビット)	xp
Windows XP (64 ビット)	xp-64

たとえば、Windows XP の Sysprep バイナリ ファイルを持つサブディレクトリを作成するには、次の Linux コマンドを使用します。

```
[root@cell1 /opt/vmware/vcloud-director/guestcustomization/default/windows]#
mkdir sysprep/xp
```

5 サーバー グループ内の各 vCloud Director サーバー上の適切な場所に Sysprep バイナリ ファイルをコピーします。

6 ユーザー **vcloud.vcloud** が Sysprep ファイルを読み込めることを確認してください。

これを実行するには、Linux **chown** コマンドを使用します。

```
[root@cell1 /]# chown -R vcloud:vcloud $VCLOUD_HOME/guestcustomization
```

サーバー グループのすべてのメンバーに Sysprep ファイルをコピーすると、クラウド内の仮想マシン上でゲストのカスタマイズを実行できます。Sysprep ファイルのコピー後に vCloud Director を再起動する必要はありません。

vCloud Director サービスの開始と停止

サーバーでのインストールとデータベース接続のセットアップを完了したら、そのサーバーで vCloud Director サービスを開始できます。実行中のサービスを停止することもできます。

構成スクリプトから、vCloud Director サービスを開始するようにメッセージが表示されます。スクリプトがサービスを自動的に開始するように設定するか、サービスを後で自分で開始することができます。インストールを完了して初期化する前に、これらのサービスを実行中の状態にしておく必要があります。

vCloud Director サービスは、サーバーを再起動すると常に開始します。

重要 vCloud Director ソフトウェア アップグレードの一部として vCloud Director サービスを停止する場合は、セルを静止してからサービスを停止できるようにするセル管理ツールを使用する必要があります。「セル管理ツールを使用したサーバーの静止とシャットダウン (P. 41)」 を参照してください。

手順

1 ターゲット サーバーにルートとしてログインします。

2 サービスを開始または停止します。

オプション	操作
サービスの開始	コンソール、シェル、またはターミナル ウィンドウを開き、次のコマンドを実行します。 `service vmware-vcd start`
セルが使用中のときに、サービスを停止します	セル管理ツールを使用します。
セルが使用中でないときには、サービスを停止します	コンソール、シェル、またはターミナル ウィンドウを開き、次のコマンドを実行します。 `service vmware-vcd stop`

vCloud Director ソフトウェアのアンインストール

個々のサーバーから vCloud Director ソフトウェアをアンインストールするには、Linux の **rpm** コマンドを使用します。

手順

1 ターゲット サーバーにルート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、rpm コマンドを実行します。

```
rpm –e vmware–vcloud–director
```

vCloud Director のアップグレード 3

vCloud Director を新しいバージョンにアップグレードするには、vCloud Director サーバー グループ内の各サーバーに新しいバージョンをインストールし、vCloud Director データベースをアップグレードして、vCloud Director サービスを再起動します。

重要　このアップグレード手順では、vCloud Director 8.0 とも互換性のある VMware vSphere およびネットワーク コンポーネント（VMware NSX for vSphere または VMware vCloud Networking and Security）を使用する vCloud Director のインストールをアップグレードするものと想定します。この手順を開始する前に、現在実行しているバージョンの vCloud Director および vCloud Director 8.0 と互換性のある他の VMware 製品のバージョン情報について、http://partnerweb.vmware.com/comp_guide/sim/interop_matrix.php の 「VMware 製品の互換性マトリックス」を参照してください。場合によっては、現在の vCloud Director インストールのいくつかのコンポーネントを vCloud Director 8.0 とも互換性のあるバージョンにアップグレードする必要があります。

---

vCloud Director サーバーのアップグレード後、その vCloud Director データベースもアップグレードする必要があります。データベースには、サーバーで実行されているすべての vCloud Director タスクの状態を含む、サーバーのランタイム状態に関する情報が保存されます。アップグレード後に無効なタスク情報がデータベース内に残らないようにするため、アップグレードを開始する前に、サーバーにアクティブなタスクがないことを確認する必要があります。

アップグレードでは、vCloud Director データベースに格納されない次のアーティファクトが保持されます。

- ローカルおよびグローバルのプロパティ ファイルは新しいインストール環境にコピーされます。
- ゲスト カスタマイズに使用する Microsoft Sysprep ファイルは、新しいインストール環境にコピーされます。

vCloud Director サーバー グループのメンバー全体にクライアントの要求を分散するのにロード バランサーを使用しない場合（「ロード バランサーを使用したサービス ダウンタイムの短縮 (P. 40)」を参照）、アップグレードには、データベースおよび少なくとも 1 つのサーバーをアップグレードするための十分な vCloud Director ダウンタイムが必要です。

vCloud Director サーバー グループのアップグレード

1. ユーザーの vCloud Director へのアクセスを無効化します。アップグレードの進行中にメンテナンス メッセージを表示することもできます。「アップグレード中のメンテナンス メッセージの表示 (P. 41)」 を参照してください。
2. セル管理ツールを使用して、サーバー グループ内のすべてのセルを静止し、各サーバー上の vCloud Director サービスをシャットダウンします。「セル管理ツールを使用したサーバーの静止とシャットダウン (P. 41)」 を参照してください。
3. サーバー グループの全メンバーの vCloud Director ソフトウェアをアップグレードします。「サーバー グループのメンバーに対する vCloud Director ソフトウェアのアップグレード (P. 43)」 を参照してください。サーバーは個別に、または並行してアップグレードできますが、vCloud Director データベースをアップグレードする前に、グループのアップグレードされたメンバー上の vCloud Director サービスを再起動してはいけません。
4. vCloud Director データベースをアップグレードします。「vCloud Director データベースのアップグレード (P. 45)」を参照してください。

5 アップグレードしたサーバーの vCloud Director を再起動します。「vCloud Director サービスの開始と停止 (P. 36)」を参照してください。

6 ユーザーの vCloud Director へのアクセスを有効化します。

7 （オプション）関連付けられた vShield Manager または NSX Manager をそれぞれアップグレードします。このサーバー グループに登録されているすべての vShield Manager または NSX Manager を、アップグレードによってインストールされるバージョンの vCloud Director と互換性のある vShield Manager または NSX Manager ソフトウェアのバージョンにアップグレードする必要があります。アップグレード プログラムによって互換性のない vShield Manager または NSX Manager のバージョンが検出された場合、アップグレードは許可されません。vCloud Director の本バージョンで導入されたネットワーク機能を使用するには、「サポート対象プラットフォーム (P. 9)」に記載されているように、 vShield Manager または NSX Manager の最新バージョンにアップグレードする必要があります。「接続された vCenter Server システムに関連付けられた既存の vShield Manager または NSX Manager のアップグレード (P. 46)」 を参照してください。

8 （オプション）関連付けられた vCenter Server システムおよびホストをそれぞれアップグレードします。「vCenter Server システム、ホスト、および vShield Edge アプライアンスのアップグレード (P. 48)」 を参照してください。このサーバー グループに登録されているすべての vCenter Server システムを、アップグレードによってインストールされるバージョンの vCloud Director と互換性のある vCenter Server ソフトウェアのバージョンにアップグレードする必要があります。互換性のない vCenter Server システムは、アップグレードの完了後に vCloud Director からアクセス不能になります。「サポート対象プラットフォーム (P. 9)」 を参照してください。

注意　アップグレードを完了した後、ブラウザで vCloud Director の Web コンソールが開いている場合は、一度ログアウトしてブラウザのキャッシュをクリアし、それから Web コンソールに再度ログインします。

ロード バランサーを使用したサービス ダウンタイムの短縮

ロード バランサーなど、要求を特定のサーバーに強制的に送信できるツールを使用している場合、サーバー グループのサブセットをアップグレードし、それ以外のサブセットでは既存のサービスをそのまま使用することができます。この方法によって、vCloud Director サービスのダウンタイムを、vCloud Director データベースのアップグレードに必要な時間の長さまで短縮できます。アップグレード中にパフォーマンスが低下する場合がありますが、サーバー グループのいずれかのサブセットが稼働中であれば、進行中のタスクは実行を継続しています。コンソール セッションは中断される場合がありますが、再起動することができます。

1 ロード バランサーを使用して、vCloud Director 要求をグループ内のサーバーのサブセットにリダイレクトします。ロード バランサーで推奨される手順に従います。

2 セル管理ツールを使用して、要求の処理を停止したセルを静止し、サーバー上の vCloud Director サービスをシャットダウンします。

注意　サーバーのコンソール プロキシを介して経路指定されたコンソール セッションは、サーバーのシャットダウン時に中断されます。クライアントがコンソール ウィンドウを更新し、回復できます。

「セル管理ツールを使用したサーバーの静止とシャットダウン (P. 41)」 を参照してください。

3 vCloud Director を停止したサーバー グループのメンバー上の vCloud Director ソフトウェアをアップグレードします。ただし、サービスは再起動しないでください。「サーバー グループのメンバーに対する vCloud Director ソフトウェアのアップグレード (P. 43)」 を参照してください。

4 セル管理ツールを使用して、まだアップグレードしていないセルを静止し、それらのサーバー上の vCloud Director サービスをシャットダウンします。

5 vCloud Director データベースをアップグレードします。「vCloud Director データベースのアップグレード (P. 45)」を参照してください。

6 アップグレードしたサーバーの vCloud Director を再起動します。「vCloud Director サービスの開始と停止 (P. 36)」を参照してください。

7 （オプション）関連付けられた vShield Manager または NSX Manager をそれぞれアップグレードします。「接続された vCenter Server システムに関連付けられた既存の vShield Manager または NSX Manager のアップグレード (P. 46)」 を参照してください。

8 （オプション）関連付けられた vCenter Server システムおよびホストをそれぞれアップグレードします。「vCenter Server システム、ホスト、および vShield Edge アプライアンスのアップグレード (P. 48)」 を参照してください。

9 ロード バランサーを使用して vCloud Director 要求をアップグレードしたサーバーにリダイレクトします。

10 グループ内の残りのサーバー上の vCloud Director ソフトウェアをアップグレードし、アップグレードが完了したらそれらのサーバー上で vCloud Director を再起動します。「サーバー グループのメンバーに対する vCloud Director ソフトウェアのアップグレード (P. 43)」 を参照してください。

アップグレード中のメンテナンス メッセージの表示

アップグレード プロセスに時間がかかることが予想され、アップグレードの進行中にメンテナンス メッセージがシステムに表示されるようにする場合は、他のセルがアップグレードされる間でも、少なくとも 1 つのセルにアクセスできることを確認してください。セルで `/opt/vmware/vcloud-director/bin/vmware-vcd-cell` コマンドを実行し、セルのメンテナンス メッセージをオンにします。

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./vmware-vcd-cell maintenance
```

アップグレードされたセルをサービスに戻す準備ができた場合は、そのセルで次のコマンドを実行してメンテナンス メッセージをオフにします。

```
[root@cell1 /opt/vmware/vcloud-director/bin]# service vmware-vcd restart
```

この章では次のトピックについて説明します。

セル管理ツールを使用したサーバーの静止とシャットダウン

vCloud Director サーバーをアップグレードする前に、セル管理ツールを使用してサーバーのセルで実行されている vCloud Director サービスを静止してシャットダウンします。

vCloud Director では、ユーザーが要求する各非同期操作を追跡および管理するためのタスク オブジェクトが作成されます。実行中および最近完了したタスクすべてに関する情報は、vCloud Director データベースに保存されます。データベースをアップグレードするとこのタスク情報が無効になるため、アップグレード プロセスを開始するときには実行中のタスクがないことを確認する必要があります。

セル管理ツールを使用すると、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てから、すべてのアクティブなタスクのステータスをチェックできます。実行中のタスクが完了するまで待機するか、または、vCloud Director にシステム管理者としてログインしてタスクをキャンセルすることができます。第 5 章「セル管理ツール リファレンス (P. 55)」 を参照してください。実行中のタスクがなくなったら、セル管理ツールを使用して vCloud Director サービスを停止できます。

開始する前に

- ターゲット サーバー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。
- vCloud Director システム管理者の認証情報があることを確認します。

- アップグレード中に vCloud Director クライアントがこのセルにアクセスできる場合、**/opt/vmware/vcloud-director/bin/vmware-vcd-cell** コマンドを使用してセルのメンテナンス メッセージをオンにしてください。

  ```
  [root@cell1 /opt/vmware/vcloud-director/bin]#
                          ./vmware-vcd-cell maintenance
  ```

  このコマンドにより、セルがメンテナンス メッセージ付きのすべてのリクエストに応答するようになります。ロード バランサーまたは類似のツールを使用してアップグレード中にはセルにアクセスできないようにしている場合、セルのメンテナンス メッセージをオンにする必要はありません。

手順

1 ターゲット サーバーにルートとしてログインします。

2 セル管理ツールを使用してセルを安全にシャットダウンします。

a 現在のジョブ ステータスを取得します。

以下の **cell-management-tool** コマンドはシステム管理者の認証情報を提供し、実行中のジョブ数を返します。

```
[root@cell1 /opt/vmware/vcloud-director/bin]#
                              ./cell-management-tool -u administrator cell --status
                                   Job count = 3 Is Active = true
```

b タスク スケジューラを停止して、セルを静止します。

以下の形式で、**cell-management-tool** コマンドを使用します。

```
[root@cell1 /opt/vmware/vcloud-director/bin]#
                                   ./cell-management-tool -u administrator cell --
quiesce true
```

このコマンドでは、新しいジョブを開始できなくします。既存のジョブは完了するか、キャンセルされるまで実行が継続します。ジョブをキャンセルするためには、vCloud Director Web コンソールまたは REST API を使用します。

c **Job count** の値 が **0** で **Is Active** の値 が **false** である場合、セルをシャットダウンしても安全です。

以下の形式で、**cell-management-tool** コマンドを使用します。

```
[root@cell1 /opt/vmware/vcloud-director/bin]#
                                   ./cell-management-tool -u administrator cell --
shutdown
```

注意 **cell-management-tool** コマンド ラインに vCloud Director システム管理者のパスワードを入力することもできますが、パスワードを省略するほうが安全です。これにより、**cell-management-tool** でパスワードが要求されるようになりますが、入力内容は画面には表示されません。

サーバーのコンソール プロキシを介して経路指定されたコンソール セッションは、サーバーのシャットダウン時に中断されます。サーバー グループのその他のメンバーがまだアクティブであれば、クライアントはコンソール ウィンドウを更新して回復できます。

次に進む前に

セル管理ツールによってこのサーバー上の vCloud Director サービスが停止されたら、サーバーの vCloud Director ソフトウェアをアップグレードしたり、サーバーが要求するその他のメンテナンスを完了させることができます。

サーバー グループのメンバーに対する vCloud Director ソフトウェアのアップグレード

vCloud Director インストーラは、ターゲット サーバー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、サーバーの vCloud Director ソフトウェアをアップグレードします。

vCloud Director ソフトウェアは、**vmware-vcloud-director-8.0.0-**<nnnnnn>**.bin** という名前の Linux 実行可能ファイルとして配布されます。<nnnnnn> はビルド番号を示します。サーバー グループのメンバーにアップグレードをインストールしたら、アップグレードしたサーバー上の vCloud Director サービスを再起動する前に、ツールを実行してグループで使用する vCloud Director データベースをアップグレードする必要があります。

開始する前に

- ターゲット サーバー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には、ターゲット サーバーに 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 (P. 25)」 を参照してください。
- セル管理ツールを使用して、サーバーのセル上の vCloud Director サービスを静止し、シャットダウンします。
- アップグレード先の vCloud Director ソフトウェアのバージョンを使用するための有効なライセンス キーがあることを確認します。

手順

1 ターゲット サーバーにルート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。

CD またはその他のメディアでソフトウェアを購入した場合、インストール ファイルをすべてのターゲット サーバーからアクセスできる場所にコピーします。

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

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

```
[root@cell1 /tmp]# md5sum <installation-file>
<checksum-value> <installation-file>
```

このコマンドで生成される <checksum-value> と、ダウンロードページからコピーした MD5 チェックサムを比較します。

4 インストール ファイルが実行可能であることを確認します。

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

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

5 セル管理ツールを使用して、セルを静止し、サーバー上の vCloud Director サービスをシャットダウンします。

「セル管理ツールを使用したサーバーの静止とシャットダウン (P. 41)」 を参照してください。

6 コンソール、シェル、またはターミナル ウィンドウで、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（**./<installation-file>** など）を入力します。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。

注意 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、このサーバーにインストールされている vCloud Director のバージョンが、インストール ファイル内のバージョン以降のものであることを検出すると、エラー メッセージを表示して終了します。バージョンが適切な場合、このサーバーのアップグレード処理を進めるかどうかを確認するメッセージが表示されます。

```
Checking architecture...done
Checking for a supported Linux distribution...done
Checking for necessary RPM prerequisites...done
Checking free disk space...done
An older version of VMware vCloud Director has been detected
```

7 アップグレード プロンプトに応答します。

オプション	操作
アップグレードを続行します。	**y** と入力します。
現在のインストール環境を変更せずに終了してシェルに戻ります。	**n** と入力します。

サーバーをアップグレードすることを確認すると、インストーラはホストがすべての要件を満たすことを確認し、vCloud Director RPM パッケージを展開し、サーバー上の vCloud Director サービスが停止してから、インストールされている vCloud Director ソフトウェアをアップグレードします。

```
Do you wish to proceed with the upgrade? (y/n)? y
Extracting vmware-vcloud-director ......done
Upgrading VMware vCloud Director...
Installing the VMware vCloud Director
Preparing...                ##################################################
vmware-vcloud-director      ##################################################
Migrating settings and files from previous release...done
Migrating in-progress file transfers to /opt/vmware/vcloud-
director/data/transfer...done
Uninstalling previous release...done
```

ターゲット サーバーに 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 サーバーの既存の **global.properties** ファイルが変更された場合、インストーラは次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
```

ほとんどのアップグレードではこの種類の変更が必要なため、この警告が表示されます。既存の **global.properties** ファイルを変更した場合は、**global.properties.rpmnew** から変更内容を取得できます。

8 (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	操作
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	`/opt/vmware/vcloud-director/etc/log4j.properties.rpmnew` ファイルを既存の `/opt/vmware/vcloud-director/etc/log4j.properties` にマージします。これらのファイルをマージすると、変更が保存されます。

vCloud Director ソフトウェアのアップグレードが完了した後、インストーラから古い構成ファイルが保存されている場所を示すメッセージと、データベース アップグレード ツールを実行するように促すメッセージが表示されます。

次に進む前に

- このサーバーで使用する vCloud Director データベースをまだアップグレードしていない場合は、アップグレードします。
- このサーバー グループで使用する vCloud Director データベースをすでにアップグレードした場合、アップグレードされたサーバーを再起動できます。「vCloud Director サービスの開始と停止 (P. 36)」 を参照してください。

vCloud Director データベースのアップグレード

vCloud Director サーバー グループ内のいずれかのサーバーをアップグレードしたら、サーバーで vCloud Director サービスを再起動する前にグループの vCloud Director データベースをアップグレードする必要があります。

vCloud Director サーバー グループ内のすべてのサーバーは同じデータベースを共有するため、アップグレードするサーバーの数に関係なく、データベースのアップグレードは一度行うだけで済みます。データベースがアップグレードされた後、vCloud Director サーバーは、それ自体もアップグレードされるまではデータベースに接続できなくなります。

開始する前に

重要　アップグレード前に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。

すべての vCloud Director セルがアクティブでないことを確認します。「セル管理ツールを使用したサーバーの静止とシャットダウン (P. 41)」 を参照してください。

手順

1 コンソール、シェル、またはターミナル ウィンドウを開き、次のコマンドを入力してデータベース アップグレード スクリプトを実行します。

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

重要　互換性のないバージョンの vShield Manager または NSX Manager が vCloud Director のこのインストールに登録されていることをデータベース アップグレード スクリプトが検出した場合は、警告メッセージが表示され、アップグレードがキャンセルされます。

```
One or more vShield Manager servers registered to this vCloud Director installation
are not supported by the version of vCloud Director you are upgrading to. Upgrade
canceled, please follow the procedures in the vShield Manager Upgrade Guide to
upgrade those unsupported vShield Manager servers.
```

2 データベース アップグレード プロンプトに応答します。

a データベース アップグレードを続行することを確認します。

```
Welcome to the vCloud Director upgrade utility This product is intended for use
only by service providers under the terms and conditions of the VMware Service
Provider Partner (VSPP) Program. If you are a member of the VSPP Program, please
locate your license key before proceeding. If you are not a member of this
program, do not proceed with this upgrade. Upgrading without a proper key will
invalidate your support contract. This utility will apply several updates to the
database.Please ensure you have created a backup of your database prior to
continuing. Do you wish to upgrade the product now?[Y/N]:
```

次のいずれかの操作を実行します。

オプション	操作
アップグレードを続行します。	**y** と入力します。
現在の vCloud Director データベースを変更せずに終了してシェルに戻ります。	**n** と入力します。

b (オプション) 必要に応じて、セルが非アクティブになるのを待機します。

いずれかのセルがアクティブのままであることがデータベース アップグレード ツールで検出された場合、ツールにアップグレードを続行するか終了するか選ぶプロンプトが表示されます。

```
Found active cell. Name: "cell-01", IP Address: 10.150.151.190, Identifier:
a2eb...
Do you wish to upgrade the database while cells are still active? [Y/N]
```

このプロンプトが表示されたら、**n** を入力してシェルを終了し、5 分間待機してからデータベース アップグレード ツールを再起動します。セルがまだアクティブであることを示す警告がデータベース アップグレード ツールにより引き続き表示される場合は、「セル管理ツールを使用したサーバーの静止とシャットダウン (P. 41)」 の手順に戻り、すべてのセルが非アクティブになったことを確認します。

すべてのプロンプトに応答すると、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。

```
Executing upgrade task: Start UpdateStatementManager ...[3] Successfully ran
upgrade task Executing upgrade task: ... .......... Successfully ran upgrade
task ... Executing upgrade task: Stop UpdateStatementManager ...[3] ...
Successfully ran upgrade task
```

データベースがアップグレードされた後は、アップグレード スクリプトによって、このホスト上で vCloud Director サービスを開始できます。

```
Would you like to start the vCloud Director service now? If you choose not to start it
now, you can manually start it at any time using this command: service vmware-vcd start
Start it now? [y/n]:y
Starting the vCloud Director service (this may take a moment). Starting vmware-vcd-
watchdog: [ OK ] Starting vmware-vcd-cell [ OK ]
```

接続された vCenter Server システムに関連付けられた既存の vShield Manager または NSX Manager のアップグレード

vCloud Director に接続された vCenter Server システムおよびホストをアップグレードする前に、この vCenter Server システムに関連付けられた vShield Manager または NSX Manager をアップグレードする必要があります。

vShield Manager または NSX Manager をアップグレードすると、vShield Manager または NSX Manager の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。

開始する前に

- アップグレードを開始する前に、vCloud Director インストール内でアップグレードされたセルが 1 つ以上実行されていることを確認します。このセルが、アップグレードされた vShield Manager または NSX Manager に関するデータを vCloud Director データベースに書き込みます。
- vShield Manager または NSX Manager のいずれをアップグレードするのかに応じて、アップグレードに必要なアイテムがあることを確認してください。

vShield Manager	NSX Manager
VMware vCloud Networking and Security ドキュメント センター (https://www.vmware.com/support/pubs/vshield_pubs.html) にあるアップグレード情報を参照してください。	NSX for vSphere ドキュメント センター (https://www.vmware.com/support/pubs/nsx_pubs.html) にあるアップグレード情報を参照してください。

手順

1 製品およびアップグレードするバージョンに適したアップグレード手順に従って、関連付けられた vShield Manager または NSX Manager インストールをアップグレードします。

注意　特定のバージョンの NSX Manager にアップグレードする場合は、関連付けられた既存の vShield Edge アプライアンスを NSX Edge アプライアンスにアップグレードしないでください。vCloud Director は NSX Edge アプライアンスをサポートしていません。NSX Manager と vCloud Director を併用している場合、vCloud Director は NSX Manager を使用して vShield Edge アプライアンスを作成します。

オプション	操作
関連付けられた vShield Manager を以降のバージョンの vShield Manager にアップグレードします。	『vShield インストールおよびアップグレード ガイド』(https://www.vmware.com/support/pubs/vshield_pubs.html) の vShield Manager のアップグレードに関する情報を参照してください。vShield Manager のみをアップグレードします。他の vShield コンポーネントはアップグレードしないでください。関連付けられた既存の vShield Edge アプライアンスはアップグレードしないでください。
関連付けられた vShield Manager を NSX Manager にアップグレードするか、関連付けられた NSX Manager を以降のバージョンの NSX Manager にアップグレードします。	『NSX インストールおよびアップグレード ガイド』(https://www.vmware.com/support/pubs/nsx_pubs.html) の NSX Manager へのアップグレードに関する情報を参照してください。vShield Manager または NSX Manager のみをアップグレードします。vShield または NSX for vSphere の他のコンポーネントはアップグレードしないでください。関連付けられた既存の vShield Edge アプライアンスはアップグレードしないでください。

2 クラウドに登録済みの他の vCenter Server システムに関連付けられた vShield Manager または NSX Manager ごとに、手順 1 を繰り返します。

アップグレードが終了すると、アップグレードされた vShield Manager または NSX Manager から vCloud Director に、ソフトウェアが新しいバージョンになったことが通知されます。通知が送信されて、vCloud Director が処理するまで、数分間かかることがあります。

次に進む前に

関連付けられた各 vShield Manager または NSX Manager をアップグレードしたら、登録済みのすべての vCenter Server システムおよびホストをアップグレードし、それから vCloud Director を使用して関連付けられた vShield Edge アプライアンスをアップグレードする必要があります。「vCenter Server システム、ホスト、および vShield Edge アプライアンスのアップグレード (P. 48)」 を参照してください。

vCenter Server システム、ホスト、および vShield Edge アプライアンスのアップグレード

vCloud Director および vShield Manager または NSX Manager をアップグレードしたら、クラウドに接続された vCenter Server システムおよびホストをアップグレードする必要があります。 接続された vCenter Server システムおよびホストをすべてアップグレードしたら、vCloud Director を使用して、Edge ゲートウェイを再展開するか、vApp ネットワークをリセットして、関連付けられた vShield Edge アプライアンスをアップグレードする必要があります。

開始する前に

クラウドに接続された vCenter Server システムに関連付けられた各 vShield Manager または 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。「接続された vCenter Server システムに関連付けられた既存の vShield Manager または NSX Manager のアップグレード (P. 46)」 を参照してください。

手順

1 接続された vCenter Server システムをアップグレードします。

『vSphere インストールおよびセットアップ ガイド』を参照してください。

2 すべての vCloud Director パブリック URL および証明書チェーンを確認します。

vCloud Director Web コンソールの [管理] タブで、左側のペインにある [公開アドレス] をクリックします。すべてのフィールドに値を入力します。

3 (オプション) vCloud Director が vCenter Single Sign On を使用するように構成した場合は、vCenter Lookup Service で vCloud Director を登録解除してから再登録する必要があります。

a ローカル アカウントまたは LDAP アカウントを使用して、システム管理者として vCloud Director にログインします。このログインでは、vCenter Single Sign On を使用しないでください。

b vCenter Lookup Service で、vCloud Director を登録解除します。

[Web コンソールの]管理 vCloud Director タブで、左側のペインの [連携] をクリックし、[登録解除] をクリックします。この操作を完了するには、適切な vCenter 管理者認証情報を提供する必要があります。

c vCenter Lookup Service で、vCloud Director を登録します。

『vCloud Director 管理者ガイド』の「vCenter Single Sign On を使用する vCloud Director の構成」を参照してください。

4 vCloud Director での vCenter Server システムの登録を更新します。

a vCloud Director Web コンソールで、[管理および監視] タブをクリックし、左側のペインで [vCenter] をクリックします。

b vCenter Server 名を右クリックし、[更新] を選択します。

c [はい] 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それぞれのホストをアップグレードします。

『vSphere インストールおよびセットアップ ガイド』を参照してください。アップグレードでは、ホストごとに次の手順を実行する必要があります。

a vCloud Director Web コンソールで、ホストを無効化します。

[管理および監視] ページで、[ホスト] をクリックし、ホストを右クリックして [ホストを無効化] を選択します。

b 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、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。

c ホストをアップグレードします。

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。

d vCenter Server システムを使用してホストを再接続します。

e ホスト上の vCloud Director ホスト エージェントをアップグレードします。

『vCloud Director 管理者ガイド』の「ESX/ESXi ホスト エージェントのアップグレード」を参照してください。

f vCloud Director Web コンソールで、ホストを有効化します。

[管理および監視] ページで、[ホスト] をクリックし、ホストを右クリックして [ホストを有効化] を選択します。

g 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 アップグレードされた vCloud Director を使用して、アップグレード済みの vCenter Server システムに関連付けられたアップグレード済みの vShield Manager または NSX Manager によって管理されているすべての vShield Edge アプライアンスをアップグレードします。

注意　アップグレードされた vCenter Server システムに、vShield Manager でなく NSX Manager が関連付けられている場合、vCloud Director による vShield Edge アプライアンスの自動アップグレードを行うには、この手順に示された方法のみを使用します。関連付けられた vShield Edge アプライアンスを NSX Edge アプライアンスにアップグレードする場合は、その他の方法を使用しないでください。vCloud Director は NSX Edge アプライアンスをサポートしていません。NSX Manager と vCloud Director を併用している場合、vCloud Director は NSX Manager を使用して vShield Edge アプライアンスを作成します。

vCloud Director Web コンソールまたは REST API のいずれかを使用して vShield Edge で保護されたネットワークをリセットすると、vShield Edge アプライアンスに適したアップグレードが自動実行されます。

- Edge ゲートウェイの場合は、Edge ゲートウェイを再展開すると、その Edge ゲートウェイに関連付けられた vShield Edge アプライアンスがアップグレードされます。
- 経路指定されている vApp ネットワーク、隔離された vApp ネットワーク、またはフェンスで囲まれた組織の仮想データセンター ネットワークなど、仮想マシンが接続されている vApp ネットワークの場合は、vApp のコンテキスト内で 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 vShield Edge アプライアンスがアップグレードされます。vCloud Director Web コンソールを使用して vApp のコンテキスト内で vApp ネットワークをリセットするには、その vApp の[ネットワーク]タブに移動し、そのネットワークの詳細を表示します。次に vApp ネットワークを右クリックして、[ネットワークをリセット]を選択します。

Edge ゲートウェイの再展開方法および vApp ネットワークのリセット方法の詳細については、使用する方法に応じて vCloud Director Web コンソールのオンライン ヘルプまたは『vCloud API プログラミング ガイド』を参照してください。

次に進む前に

この手順を、クラウドに登録された他の vCenter Server システムについて繰り返します。

vCloud Director セットアップ 4

vCloud Director サーバー グループ内のすべてのサーバーを構成して、データベースに接続したら、ライセンス キー、システム管理者アカウント、および関連情報を使用してサーバー グループのデータベースを初期化できます。このプロセスの完了後、vCloud Director Web コンソールを使用してクラウドの初期プロビジョニングを完了できます。

vCloud Director Web コンソールを実行する前に、セットアップ ウィザードを実行する必要があります。このウィザードでは Web コンソールが開始するのに必要な情報が収集されます。ウィザードが終了すると、Web コンソールが開始し、ログイン画面が表示されます。vCloud Director Web コンソールでは、クラウドのプロビジョニングと管理のための一連のツールを提供します。これには、vCloud Director を vCenter に関連付けて組織を作成する手順を説明する Quickstart (クイックスタート) 機能も含まれます。

開始する前に

- すべての vCloud Director サーバーのインストールを完了し、vCloud Director サービスがすべてのサーバー上で開始したことを確認します。
- 構成スクリプトの完了時に表示される URL が手元にあることを確認します。

  注意　スクリプトが終了した後にセットアップ ウィザードの URL を特定するには、最初のサーバーのインストール時に HTTP サービスに指定した IP アドレスに関連付けられた完全修飾ドメイン名を見つけ、そのドメイン名を使用して https://<fully-qualified-domain-name> の形式の URL (https://mycloud.example.com など) を作成します。この URL からウィザードに接続できます。

すべての vCloud Director サーバーのインストールを完了し、vCloud Director サービスがすべてのサーバー上で開始したことを確認します。

手順

1 Web ブラウザを開き、構成スクリプトの完了時に表示される URL に接続します。

  注意　場合によっては、vCloud Director サービスを起動した後、セットアップ ウィザードまたは Web コンソールの準備ができるまで数分間待機する必要があります。

2 案内に従ってセットアップを完了します。

この章では次のトピックについて説明します。

使用許諾契約書の確認

vCloud Director サーバー グループを構成する前に、エンド ユーザー使用許諾契約書を確認して同意する必要があります。

手順

1 使用許諾契約書を確認します。

2 契約書に同意するか、拒否します。

オプション	操作
使用許諾契約書に同意する場合は、	[はい、使用許諾契約書に同意します。] をクリックします。
使用許諾契約書を拒否する場合は、	[いいえ、使用許諾契約書に同意しません。] をクリックします。

使用許諾契約書を拒否した場合、vCloud Director の構成に進むことはできません。

ライセンス キーの入力

各 vCloud Director クラスタを実行するにはライセンスが必要です。ライセンスは製品シリアル番号として指定します。製品シリアル番号は vCloud Director データベースに保存されます。

vCloud Director 製品シリアル番号は、vCenter Server のライセンス キーとは異なります。vCloud を動作させるには、vCloud Director の製品シリアル番号と vCenter Server のライセンスキーが必要です。両方のタイプのライセンス キーを VMware ライセンス ポータルから取得できます。

手順

1 vCloud Director の製品シリアル番号を VMware ライセンス ポータルから取得します。

2 [製品シリアル番号] テキスト ボックスに製品シリアル番号を入力します。

システム管理者アカウントの作成

vCloud Director システム管理者のユーザー名、パスワード、および連絡先情報を指定します。

vCloud Director システム管理者には、クラウド全体に対するスーパーユーザー権限があります。最初のシステム管理者アカウントは、vCloud Director のセットアップ中に作成します。インストールと構成が完了したら、このシステム管理者が必要に応じて追加のシステム管理者を作成できます。

手順

1 システム管理者のユーザー名を入力します。

2 システム管理者のパスワードを入力して確認します。

3 システム管理者のフル ネームを入力します。

4 システム管理者の電子メール アドレスを入力します。

システム設定の指定

vCloud Director と vSphere と vShield Manager または NSX Manager 間の連携方法を制御するシステム設定を指定できます。

構成プロセスでは、vCloud Director で使用するフォルダを接続先の vCenter Server システム内に作成して、仮想 NIC 用の MAC アドレスを作成するときに使用するインストール ID を指定します。

手順

1 vCloud Director システム名[フィールドに] vCenter Server フォルダの名前を入力します。

2 [インストール ID] フィールドを使用して、この vCloud Director インストール環境のインストール ID を指定します。

データセンターに複数の vCloud Director インストール環境が含まれる場合、各インストール環境に一意のインストール ID を指定する必要があります。

vCloud Director へのログイン準備完了

セットアップ ウィザードで必要な情報をすべて指定したら、設定を確認してウィザードを完了できます。ウィザードが終了すると、vCloud Director Web コンソールのログイン画面が表示されます。

ログイン準備完了ページに、ウィザードで指定した設定がすべて表示されます。設定を注意深く確認してください。

開始する前に

クラウドで使用する vCenter Server システム、およびこの vCenter Server システムに関連付けられた vShield Manager または NSX Manager にアクセスできることを確認します。vCloud Director Web コンソールには、vCloud Director インストールの一部として構成する vCenter Server および vShield Manager または NSX Manager のインストール環境へのアクセス権限が必要です。このタスクを終了するには、これらのインストール環境が稼働中であり、互いに連動するように構成されている必要があります。構成要件の詳細については、「vCloud Director のハードウェアおよびソフトウェア要件 (P. 9)」 を参照してください。

手順

- 設定を変更するには、設定を行ったページが表示されるまで [戻る] をクリックします。
- すべての設定を確認し、構成プロセスを完了するには、[終了] をクリックします。

[終了] をクリックすると、指定した設定がウィザードによって適用され、vCloud Director Web コンソールが開始してログイン画面が表示されます。

次に進む前に

システム管理者アカウントに指定したユーザー名とパスワードを使用して、表示されたログイン画面から vCloud Director Web コンソールにログインします。ログインすると、コンソールに一連の Quickstart (クイックスタート) 手順が表示されます。このクラウドを使用するには、この手順を実行する必要があります。手順を完了すると、ガイドされたタスクが有効になり、クラウドが使用できる状態になります。

セル管理ツール リファレンス 5

セル管理ツールは、セルおよびその SSL 証明書を管理し、vCloud Director データベースからテーブルをエクスポートするために使用することができるコマンドライン ユーティリティです。一部の操作には、スーパーユーザーまたはシステム管理者の証明書が必要です。

セル管理ツールは、`/opt/vmware/vcloud-director/bin/cell-management-tool` にインストールされます。

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
```

例: セル管理ツールの使用法のヘルプ

```
[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
ciphers - Reconfigure the list of disallowed SSL ciphers for the cell
configure-metrics - Collects and stores properties necessary for collecting and
querying metrics data
dbextract - Exports the data from the given set of tables
fix-scheduler-data - Scan database for corrupt scheduler data.  Fix scheduler job data
if corrupt.
generate-certs - Generates self-signed SSL certificates for use with vCD cell.
recover-password - Change a forgotten System Administrator password. Database
credentials are required.
fail-tasks - Fail all tasks running on this cell and set a custom failure message.

For command specific help:
 cell-management-tool <commandName> -h
```

- セルの管理 (P. 56)

  セル管理ツールの `cell` 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チェックしたり、セルのメンテナンス モードをコントロールしたり、セルを安全にシャットダウンしたりすることができます。

- データベース テーブルのエクスポート (P. 57)
  セル管理ツールの **dbextract** コマンドを使用すると、vCloud Director データベースからデータをエクスポートできます。
- 破損したスケジューラ データの検出および修復 (P. 60)
  vCloud Director データベースのユーザー名およびパスワードがわかっている場合は、セル管理ツールの **fix-scheduler-data** コマンドを使用して破損したスケジュール データがないかデータベース内をスキャンし、必要に応じてそのデータを修復できます。
- SSL 証明書の置換 (P. 60)
  セル管理ツールの **certificates** コマンドを使用すると、セルの SSL 証明書を置換できます。
- 自己署名 SSL 証明書の生成 (P. 61)
  セル管理ツールの **generate-certs** コマンドを使用すると、セルの新しい自己署名付き SSL 証明書を生成できます。
- 許可された SSL 暗号のリストの管理 (P. 63)
  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 (P. 64)
  SSL ハンドシェイク プロセス中にセルが使用を提案する SSL プロトコルのセットを構成するには、セル管理ツールの **ssl-protocols** コマンドを使用します。
- メトリック データベース接続の構成 (P. 65)
  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 **configure-metrics** 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 (P. 66)
  vCloud Director データベースのユーザー名とパスワードが分かっている場合は、セル管理ツールの **recover-password** コマンドを使用して、vCloud Director システム管理者のパスワードを復元できます。
- タスクの失敗ステータスの更新 (P. 67)
  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。

セルの管理

セル管理ツールの **cell** 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チェックしたり、セルのメンテナンス モードをコントロールしたり、セルを安全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 -u <sysadmin-username> -p <sysadmin-password> cell <command>
```

<sysadmin-username> vCloud Director システム管理者のユーザー名。

<sysadmin-password> vCloud Director システム管理者のパスワード。

> 注意 **cell-management-tool** コマンド ラインに vCloud Director システム管理者のパスワードを入力することもできますが、パスワードを省略するほうが安全です。これにより、**cell-management-tool** でパスワードが要求されるようになりますが、入力内容は画面には表示されません。

<command> **cell** サブコマンド。

表 5-1. セル管理ツールのオプションと引数、 cell サブコマンド

コマンド	引数	説明
--help (-h)	なし	このカテゴリで使用可能なコマンドの概要を示します。
--maintenance (-m)	true または false	セルのメンテナンス モードをコントロールします。引数 true により、セルがメンテナンス モードになります。(まずセルを静止する必要があります。)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。
--quiesce (-q)	true または false	セル上のアクティビティを静止します。引数 true はスケジューラを中断します。引数 false はスケジューラを再開します。
--shutdown (-s)	なし	サーバー上の vCloud Director サービスをシャットダウンします。
--status (-t)	なし	セル上で実行されているタスクの数とセルのステータスに関する情報を表示します。
--status-verbose (-tt)	なし	セル上で実行されているタスクとセルのステータスに関する詳細情報を表示します。

例: タスク ステータスの取得

以下の cell-management-tool コマンド ラインはシステム管理者の認証情報を提供し、実行中のタスク数を返します。Job count の値が 0 で Is Active の値が false である場合、セルをシャットダウンしても安全です。

```
[root@cell1 /opt/vmware/vcloud-
director/bin]# ./cell-management-tool -u administrator cell --status
Job count = 3 Is Active = true In Maintenance Mode = false
```

データベース テーブルのエクスポート

セル管理ツールの dbextract コマンドを使用すると、vCloud Director データベースからデータをエクスポートできます。

データベース テーブルをエクスポートするには、次の形式でコマンドラインを使用します。

```
cell-management-tool dbextract <options>
```

表 5-2. セル管理ツールのオプションと引数、 dbextract 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。
-categories	エクスポートするテーブル カテゴリのカンマ区切りリスト。	任意。NETWORKING が唯一サポートされているカテゴリです。
-dataFile	エクスポートするデータを記述したファイルへの絶対パス。	任意。指定しない場合、このコマンドでは $VCLOUD_HOME/etc/data_to_export.properties が使用されます。「エクスポートするテーブルと列の指定 (P. 59)」 を参照してください。

表 5-2. セル管理ツールのオプションと引数、 dbextract サブコマンド (続き)

オプション	引数	説明
-dumpFolder	ダンプを作成するフォルダの絶対パス。フォルダは存在していて、vCloud から書き込み可能である必要があります。	すべてのデータはこのフォルダ内のファイルにエクスポートされます。
-exportSettingsFile	データ エクスポート設定プロパティ ファイルへの絶対パス。	任意。指定しない場合、このコマンドでは $VCLOUD_HOME/etc/data_export_settings.ini が使用されます。「エクスポートする行の制限と順序 (P. 59)」 を参照してください。
-properties	データベース接続プロパティ ファイルへの絶対パス。	任意。指定しない場合、このコマンドでは、$VCLOUD_HOME/etc/global.properties のデータベース接続プロパティが使用されます。「プロパティ ファイルの指定 (P. 58)」 を参照してください。
-tables	テーブルのカンマ区切りリスト。	任意。個々のテーブル名がわかるようにしてすべてのテーブルをエクスポートします。

プロパティ ファイルの指定

デフォルトで dbextract コマンドは、現在のセルの $VCLOUD_HOME/etc/global.properties ファイルにあるデータベース接続情報を使用して vCloud Director データベースからデータを抽出します。別の vCloud Director データベースからデータを抽出するには、ファイルでデータベース接続プロパティを指定し、コマンドラインで -properties オプションを使用してそのファイルへのパス名を指定します。プロパティ ファイルは、次の形式に従う UTF-8 ファイルです。

```
username=<username>
password=<password>
servicename=<db_service_name>
port=<db_connection_port>
database-ip=<db_server_ip_address>
db-type=<db_type>
```

<username>	vCloud Director データベースのユーザー名。
<password>	vCloud Director データベースのパスワード。
<db_service_name>	データベース サービス名。たとえば、orcl.example.com。
<db_connection_port>	データベース ポート。
<db_server_ip_address>	データベース サーバーの IP アドレス。
<db_type>	データベース タイプ。Oracle または MS_SQL にする必要があります。

エクスポートするテーブルと列の指定

エクスポートするデータ セットを制限するには、**–exportSettingsFile** オプションを使用し、エクスポートする個々のテーブルと、任意で各列を指定する **data_to_export.properties** ファイルを作成します。このファイルは、行を何も含まないか、<TABLE_NAME>:<COLUMN_NAME> 形式の行を含んだ UTF-8 ファイルです。

<TABLE_NAME>	データベース内のテーブルの名前。テーブル名の一覧を表示するには、すべてのテーブルをエクスポートします。
<COLUMN_NAME>	指定した <TABLE_NAME> 内の列の名前。

このサンプルの **data_to_export.properties** ファイルでは、**ACL** テーブルと **ADDRESS_TRANSLATION** テーブルから列をエクスポートします。

```
ACL:ORG_MEMBER_ID
ACL:SHARABLE_ID
ACL:SHARABLE_TYPE
ACL:SHARING_ROLE_ID
ADDRESS_TRANSLATION:EXTERNAL_ADDRESS
ADDRESS_TRANSLATION:EXTERNAL_PORTS
ADDRESS_TRANSLATION:ID
ADDRESS_TRANSLATION:INTERNAL_PORTS
ADDRESS_TRANSLATION:NIC_ID
```

このコマンドでは、このファイルが **$VCLOUD_HOME/etc/data_to_export.properties** に存在すると想定していますが、別のパスを指定することもできます。

エクスポートする行の制限と順序

どのテーブルの場合でも、エクスポートする行の数とエクスポートされる行の順序を指定できます。**–exportSettingsFile** オプションを使用し、個々のテーブルを指定する **data_export_settings.ini** ファイルを作成します。このファイルは、エントリが何もないか、次の形式のエントリを含んだ UTF-8 ファイルです。

```
[<TABLE_NAME>]
rowlimit=<int>
orderby=<COLUMN_NAME>
```

<TABLE_NAME>	データベース内のテーブルの名前。テーブル名の一覧を表示するには、すべてのテーブルをエクスポートします。
<COLUMN_NAME>	指定した <TABLE_NAME> 内の列の名前。

このサンプルの **data_export_settings.ini** では、**AUDIT_EVENT** テーブルからエクスポートされるデータを先頭の 10000 行に制限し、**event_time** 列の値を基準に行の順序を指定しています。

```
[AUDIT_EVENT]
rowlimit=100000
orderby=event_time
```

このコマンドでは、このファイルが **$VCLOUD_HOME/etc/data_export_settings.ini** に存在すると想定していますが、別のパスを指定することもできます。

例: 現在の vCloud Director データベースからのすべてのテーブルのエクスポート

この例では、現在の vCloud Director データベースから /tmp/dbdump ファイルにすべてのテーブルをエクスポートします。

```
[root@cell1 /opt/vmware/vcloud-director/bin]#
./cell-management-tool dbextract -dumpFolder /tmp/dbdump
This utility outputs data from your vCloud Director system that may
contain sensitive data. Do you want to continue and output the data (y/n)?
y
Exporting data now. Please wait for the process to finish Exported 144
of 145 tables.
```

破損したスケジューラ データの検出および修復

vCloud Director データベースのユーザー名およびパスワードがわかっている場合は、セル管理ツールの **fix-scheduler-data** コマンドを使用して破損したスケジュール データがないかデータベース内をスキャンし、必要に応じてそのデータを修復できます。

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 5-3. セル管理ツールのオプションと引数、 **fix-scheduler-data** サブコマンド

オプション	引数	説明
--help (-h)	なし	このカテゴリで使用可能なコマンドの概要を示します。
--dbuser	vCloud Director データベース ユーザーのユーザー名。	コマンドラインで指定する必要があります。
--dbpassword	vCloud Director データベース ユーザーのパスワード。	指定しない場合に入力が求められます。

SSL 証明書の置換

セル管理ツールの **certificates** コマンドを使用すると、セルの SSL 証明書を置換できます。

セル管理ツールの **certificates** コマンドにより、セルの既存証明書を JCEKS キーストアに保存されている新しい証明書で置換するプロセスが自動化されます。**certificates** コマンドにより、自己署名付き証明書を署名付き証明書で置換することができます。署名付き証明書を保存する JCEKS キーストアを作成するには、「署名付き SSL 証明書の作成とインポート (P. 18)」を参照してください。

セルの SSL 証明書を置換するには、次の形式でコマンドを使用します。

```
cell-management-tool certificates <options>
```

表 5-4. 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
--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。
--config (-c)	セルの global.properties ファイルへのフル パス名	デフォルトで $VCLOUD_HOME/etc/global.properties です。
--httpks (-j)	なし	HTTP エンドポイントで使用する certificates という名前のキーストア ファイルを生成します。
--consoleproxyks (-p)	なし	コンソール プロキシ エンドポイントで使用する proxycertificates という名前のキーストア ファイルを生成します。
--responses (-r)	セルの responses.properties ファイルへのフル パス名	デフォルトで $VCLOUD_HOME/etc/responses.properties です。
--keystore (-k)	<keystore-pathname>	署名付き証明書が保存されている JCEKS キーストアへのフル パス名です。-k に置き換えられる非推奨の -s 短縮形
--keystore-password (-w)	<keystore-password>	--keystore オプションによって参照される JCEKS キーストアのパスワードです。非推奨の -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@cell1 /opt/vmware/vcloud-
director/bin]# ./cell-management-tool certificates -j -k /tmp/my-new-certs.ks -w kspw
Certificate replaced by user specified keystore at /tmp/new.ks. You will need to
restart the cell for changes to take effect.
```

注意　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。

自己署名 SSL 証明書の生成

セル管理ツールの generate-certs コマンドを使用すると、セルの新しい自己署名付き SSL 証明書を生成できます。

セル管理ツールの generate-certs コマンドにより、「自己署名付き SSL 証明書の作成 (P. 21)」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 5-5. 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)	< days-until-expiration>	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)	<name>=<value> [, <name>=<value>, ...]	証明書発行者の X.509 識別名。デフォルトでは CN=<FQDN> です。<FQDN> はセルの完全修飾ドメイン名です。完全修飾ドメイン名が使用できない場合は、その IP アドレスです。複数の属性と値のペアを指定する場合は、各ペアをカンマで区切り、引数全体を引用符で囲んでください。
--httpcert (-j)	なし	HTTP エンドポイントの証明書を生成します。
--key-size (-s)	<key-size>	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、1024 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)	<keystore-password>	このホスト上のキーストアのパスワードです。
--out (-o)	<keystore-pathname>	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生成します。

注意　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、デフォルトを使用して新しい証明書を作成します。発行者名は CN=Unknown に設定されています。証明書はキー長にデフォルトの 2048 ビットを使用し、作成後 1 年で期限切れになります。

```
[root@cell1 /opt/vmware/vcloud-director/bin]#
                    ./cell-management-tool generate-certs -j -p -o /tmp/cell.ks -w kspw
                    New keystore created and written to /tmp/cell.ks.
```

この例では HTTP エンドポイント専用の新しい証明書を作成します。また、キー サイズおよび発行者名を示すカスタム値を指定します。発行者名は CN=Test, L=London, C=GB に設定されています。HTTP 接続の新しい証明書のキー長は 4096 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.
```

許可された SSL 暗号のリストの管理

SSL ハンドシェイク プロセス中に使用するためにセルが提供する暗号化スイートのセットを構成するには、セル管理ツールの **ciphers** コマンドを使用します。

クライアントが vCloud Director セルとの SSL 接続を確立すると、セルはデフォルトの許可暗号リスト上で構成された暗号のみを使用するよう提案します。接続を保護する十分な強度がないか、あるいは SSL 接続障害の原因となることがわかっているために、このリストに含まれていない暗号があります。vCloud Director をインストールまたはアップグレードすると、インストールまたはアップグレードのスクリプトがセルの証明書を調べます。いずれかの証明書が許可暗号リストに含まれていない暗号を使用して暗号化されている場合、スクリプトはセルの構成を変更してこの暗号の使用を許可し、警告を表示します。これらの暗号を利用しながら既存の証明書を引き続き使用することも、次の手順を実行して証明書を置き換え、許可暗号リストを再構成することもできます。

1 禁止されたどの暗号も使用しない新しい証明書を作成します。「例: 許可されているすべての暗号の一覧表示 (P. 64)」に示された **cell-management-tool ciphers -a** を使用して、デフォルト構成で許可されている暗号をすべて一覧表示することができます。

2 **cell-management-tool certificates** コマンドを使用すると、セルの既存の証明書が新しい証明書で置き換えられます。

3 **cell-management-tool ciphers** コマンドを使用すると、許可暗号リストを再構成して、新しい証明書で使用されない暗号を除外することができます。これらの暗号を除外すると、ハンドシェイク中に提供される暗号数が実用的な最小数まで減るため、セルとの SSL 接続を確立するまでの時間が短縮されます。

重要 VMRC コンソールでは AES256-SHA および AES128-SHA 暗号を使用する必要があるため、vCloud Director クライアントで VMRC コンソールを使用する場合は、これらを禁止できません。

許可されている SSL 暗号のリストを管理するには、次の形式のコマンド ラインを使用します。

```
cell-management-tool
                    ciphers
                    <options>
```

表 5-6. 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
--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。
--all-allowed (-a)	なし	許可されているすべての暗号を一覧表示します。
--compatible-reset (-c)	なし	デフォルトの許可暗号リストにリセットし、さらにこのセルの証明書で使用される暗号を許可します。
--disallow (-d)	http://www.openssl.org/docs/apps/ciphers.html で公開されている、暗号名のカンマ区切りリスト	指定されたカンマ区切りリストで暗号を禁止します。
--list (-l)	なし	現在構成されている暗号を一覧表示します。
--reset (-r)	なし	デフォルトの許可暗号リストにリセットします。このセルの証明書で禁止された暗号が使用されている場合は、許可された暗号を使用する新しい証明書をインストールするまで、このセルとの SSL 接続は確立できません。

例: 許可されているすべての暗号の一覧表示

`--all-allowed` (-a) オプションを使用すると、このセルが SSL ハンドシェイク中に提供することが許可されている暗号がすべて一覧表示されます。

```
[root@cell1 /opt/vmware/vcloud-director/bin]#
                ./cell-management-tool ciphers -a
                * TLS_DHE_DSS_WITH_AES_256_CBC_SHA * TLS_DHE_DSS_WITH_AES_128_CBC_SHA
* TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA * TLS_DHE_RSA_WITH_AES_256_CBC_SHA *
TLS_DHE_RSA_WITH_AES_128_CBC_SHA * TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA *
TLS_RSA_WITH_AES_256_CBC_SHA * TLS_RSA_WITH_AES_128_CBC_SHA *
TLS_RSA_WITH_3DES_EDE_CBC_SHA * TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA *
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA * TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA *
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA * TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA *
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA * TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA *
TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA * TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA *
TLS_ECDH_RSA_WITH_AES_256_CBC_SHA * TLS_ECDH_RSA_WITH_AES_128_CBC_SHA *
TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA * SSL_RSA_WITH_3DES_EDE_CBC_SHA *
SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA
```

例: 2 つの暗号の禁止

許可暗号リストから 1 つ以上の暗号を削除するには、`--disallow` (-d) オプションを使用します。このオプションには 1 つ以上の暗号名を指定する必要があります。 カンマ区切りリストでは、複数の暗号名を指定できます。`ciphers -a` の出力からこのリストの名前を取得できます。次の例では、前の例で一覧表示された 2 つの暗号を削除します。

```
[root@cell1 /opt/vmware/vcloud-director/bin]#
                ./cell-management-tool ciphers -d
SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA,SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA
```

許可された SSL プロトコルのリストの管理

SSL ハンドシェイク プロセス中にセルが使用を提案する SSL プロトコルのセットを構成するには、セル管理ツールの `ssl-protocols` コマンドを使用します。

クライアントが vCloud Director セルとの SSL 接続を確立すると、セルは許可された SSL プロトコルのリスト上で構成されたプロトコルのみを使用するよう提案します。SSLv3 や SSLv2Hello などのプロトコルには重大なセキュリティ上の脆弱性があることがわかっているため、デフォルトのリストには含まれていません。

許可されている SSL プロトコルのリストを管理するには、次の形式のコマンド ラインを使用します。

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

表 5-7. 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
`--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。
`--all-allowed` (-a)	なし	vCloud Director がサポートできるすべての SSL プロトコルをリストします。
`--disallow` (-d)	SSL プロトコル名のコンマ区切りのリスト	許可されない SSL プロトコルのリストを、リスト内で指定されたプロトコルに再構成します。

表 5-7. 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
--list (-l)	なし	vCloud Director が現在サポートするように構成されている、許可された SSL プロトコルのセットをリストします。
--reset (-r)	なし	構成された SSL プロトコルのリストを出荷時のデフォルトにリセットします。

重要 **ssl-protocols --disallow** または **ssl-protocols reset** を実行した後は、セルを再起動する必要があります。

例: 許可され構成された SSL プロトコルの一覧表示

--all-allowed (-a) オプションを使用すると、このセルが SSL ハンドシェイク中に提供することが許可されている SSL プロトコルがすべて一覧表示されます。

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./cell-management-tool ssl-protocols -a
製品のデフォルトの SSL プロトコル: TLSv1.2 TLSv1.1 TLSv1 SSLv3 SSLv2Hello
```

このリストは通常、セルがサポートするように構成された SSL プロトコルのスーパーセットです。これらの SSL プロトコルを一覧表示するには、--list (-l) オプションを使用します。

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./cell-management-tool ssl-protocols -l
許可された SSL プロトコル: TLSv1.2 TLSv1.1 TLSv1
```

例: 許可されない SSL プロトコルのリストの再構成

--disallow (-d) オプションを使用すると、許可されない SSL プロトコルのリストが再構成されます。 このオプションを使用するには、ssl-protocols -a によって生成された許可されるプロトコルのサブセットのコンマ区切りのリストが必要です。

この例では、許可された SSL プロトコルのリストから TLSv1 SSL プロトコルを削除します。

```
[root@cell1 /opt/vmware/vcloud-
director/bin]# ./cell-management-tool ssl-protocols -d TLSv1,SSLv3,SSLv2Hello
```

このコマンドを実行した後は、セルを再起動する必要があります。

メトリック データベース接続の構成

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 configure-metrics コマンドを使用します。

vCloud Director は、仮想マシンのパフォーマンスおよびリソース消費に関する現在および過去の情報を提供するメトリックを収集できます。履歴メトリックのデータは Cassandra でバッキングされる KairosDB データベースに格納されます。第 6 章「過去の仮想マシン パフォーマンス メトリックを格納および取得するためのオプション データベース ソフトウェアのインストールと構成 (P. 69)」 を参照してください。

KairosDB から vCloud Director への接続を作成するには、次の形式のコマンド ラインを使用します。

```
cell-management-tool configure-metrics <options>
```

表 5-8. セル管理ツールのオプションと引数、 configure-metrics サブコマンド

コマンド	引数	説明
--help (-h)	なし	このカテゴリで使用可能なコマンドの概要を示します。
--repository-host	KairosDB ホストのホスト名または IP アドレス	KairosDB が複数インストールされている場合は、ロード バランサーのアドレスをここに指定する必要があります。
--repository-port	使用する KairosDB ポート。	デフォルトでは、KairosDB はポート 8080 でリスンします。

例: メトリック データベース接続の構成

この例では、IP アドレス 10.0.0.1 にホストされている KairosDB インスタンスをデフォルト ポートで使用するようにシステムを構成します。アドレスには KairosDB の単一インスタンスを実行している単一マシンのアドレス、または要求を KairosDB の複数のインスタンスに分配するロード バランサーのアドレスのいずれかを指定できます。

```
[root@cell1 /opt/vmware/vcloud-
director/bin]#
./cell-management-tool configure-metrics --repository-host 10.0.0.1 --repository-port
8080
```

システム管理者のパスワードの復元

vCloud Director データベースのユーザー名とパスワードが分かっている場合は、セル管理ツールの recover-password コマンドを使用して、vCloud Director システム管理者のパスワードを復元できます。

セル管理ツールの recover-password コマンドでは、vCloud Director データベースのユーザー名とパスワードを知っているユーザーが、vCloud Director システム管理者のパスワードを復元できます。

システム管理者のパスワードを復元するには、次の形式でコマンドラインを使用します。

```
cell-management-tool
                    recover-password
                    <options>
```

表 5-9. セル管理ツールのオプションと引数、 recover-password サブコマンド

オプション	引数	説明
--help (-h)	なし	このカテゴリで使用可能なコマンドの概要を示します。
--dbuser	vCloud Director データベース ユーザーのユーザー名。	コマンドラインで指定する必要があります。
--dbpassword	vCloud Director データベース ユーザーのパスワード。	指定しない場合に入力が求められます。

タスクの失敗ステータスの更新

セルが意図的にシャットダウンされたときに実行していたタスクに関連する完了ステータスを更新するには、セル管理ツールの **fail-tasks** コマンドを使用します。すべてのセルをシャットダウンしない限り、**fail-tasks** コマンドを使用することはできません。

cell-management-tool -q コマンドを使用してセルを静止すると、実行中のタスクは数分以内に安全に終了します。休止したセルでタスクが実行し続ける場合、スーパーユーザーはセルをシャットダウンすることができ、その結果実行しているタスクは失敗します。シャットダウンにより実行中のタスクが失敗した後、スーパーユーザーは**cell-management-tool fail-tasks** を実行してそれらのタスクの完了ステータスを更新することができます。これはタスクの完了ステータスを更新するオプションの方法ですが、管理アクションによって発生した失敗を明確に特定できるため、システムの整合性を維持するのに役立ちます。

休止したセルで実行し続けるタスクのリストを生成するには、次の形式でコマンドラインを使用します。

```
cell-management-tool -u <sysadmin-username> cell --status-verbose
```

表 5-10. セル管理ツールのオプションと引数、 **fail-tasks** サブコマンド

コマンド	引数	説明
--help (-h)	なし	このカテゴリで使用可能なコマンドの概要を示します。
--message (-m)	メッセージ テキスト。	タスク完了ステータスに含めるメッセージ テキスト。

例: セルで実行中のタスクの終了

この例では、セルがシャットダウンされた時に実行していたタスクに関連するタスク完了ステータスを更新します。

```
[root@cell1 /opt/vmware/vcloud-
director/bin]# ./cell-management-tool fail-tasks -m "administrative shutdown"
Operation: IMPORT_SINGLETON_VAPP, Start time: 12/16/13 6:41 PM, Username: system,
Organization: org1 Would you like to fail the tasks listed above?
```

「**y**」を入力すると、タスクが更新され、**管理シャットダウン**のステータスが完了になります。「**n**」と入力すると、タスクの実行を継続できます。

注意　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。

過去の仮想マシン パフォーマンス メトリックを格納および取得するためのオプション データベース ソフトウェアのインストールと構成

6

vCloud Director は仮想マシンのパフォーマンスやクラウド内の仮想マシンのリソース消費量に関する現在および過去の情報を示すメトリックを収集できます。履歴メトリックのデータは Cassandra クラスタでバッキングされる KairosDB データベースに格納されます。

Cassandra および KairosDB はオープン ソース データベースです。これらを同時に展開すると、仮想マシンのメトリックのような時系列データを収集できる、拡張性に優れたハイパフォーマンスなソリューションを実現できます。クラウド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には、Cassandra および KairosDB をインストールおよび構成してから、`cell-management-tool` ユーティリティを使用して vCloud Director を KairosDB 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。

履歴メトリックの取得をサポートするには、vCloud Director に Cassandra クラスタが必要です。Cassandra クラスタは、Cassandra がインストールされていて、Cassandra サービスが実行されている 1 台以上のマシンで構成されています。標準的な vCloud Director インストールでは、Cassandra クラスタ内に少なくとも 3 台のマシンが必要です。vCloud Director メトリックの監視機能では複製係数に 2 が使用されるため、Cassandra クラスタ内に 3 台のマシン（ノード）があると、1 台のノードをトランザクションの処理に常に使用できます。vCloud Director インストールでは単一の Cassandra クラスタを使用できます。

Cassandra クラスタと連携するように構成された KairosDB のインスタンスも 1 つ以上必要です。クラウドが多数の仮想マシンから履歴メトリックを収集する場合は、追加の KairosDB インスタンスが必要になることがあります。いずれかの Cassandra ノードに KairosDB をインストールおよび構成して、セル管理ツールをこのエンドポイントに指定するか、あるいは Cassandra ノードごとに KairosDB をインストールおよび構成し、構成の前面にロード バランサーを追加して、セル管理ツールをロード バランサーのエンドポイントに指定することができます。vCloud Director は単一の IP アドレスで KairosDB と通信することを想定されているため、KairosDB の複数のインスタンスが含まれているインストール環境ではロード バランサーを使用して、これらのアドレスの提供と vCloud Director 要求の KairosDB インスタンスへの分配を行う必要があります。

開始する前に

- オプションのデータベース ソフトウェアを構成する前に、vCloud Director がインストールおよび実行されていることを確認します。
- Cassandra および KairosDB にまだ慣れていない場合は、http://cassandra.apache.org/ および https://code.google.com/p/kairosdb/ で入手可能な資料を確認してください。
- Cassandra 1.2.<x> または Cassandra 2.0.<x> を http://cassandra.apache.org/download/ から取得します。
- KairosDB 0.9.1 を https://code.google.com/p/kairosdb/ から取得します。
- この構成に従って、vCloud Director インストールで使用する予定の Cassandra クラスタのインストールと構成を完了します。
  - Cassandra 1.2.<x> または Cassandra 2.0.<x> は、vCloud Director セルで使用しているのと同じネットワークに接続された 3 台以上のマシンにインストールされています。
  - これらのマシンは、共有ストレージでなく、独自の物理ストレージを持つように構成されています。

  - マシンは Cassandra クラスタとして構成されています。
  - Cassandra クラスタでは、メモリ使用およびディスク アクセスのパフォーマンスを高めるために Java Native Access (JNA) バージョン 3.2.7 以降が有効になっています。
- Cassandra クラスタをデータベースとして使用するために、いずれかの Cassandra ノードで KairosDB 0.9.1 の 1 つ以上のインスタンスのインストールおよび構成を完了します。この構成の前面にロード バランサーを追加する場合は、各 Cassandra ノードに KairosDB をインストールおよび構成することもできます。
- KairosDB および Cassandra が正しく構成されていることを確認します。Web ブラウザを使用して、`http://<KairosDB-IP>:8080/api/v1/metricnames` を参照します。ページを開いてもエラーが発生しない場合、KairosDB および Cassandra は正しく構成されています。
- `cell-management-tool` ユーティリティの `service` コマンドを実行できることを確認します。`service` コマンドの詳細については、「vCloud Director サービスの開始と停止 (P. 36)」を参照してください。

手順

1 `cell-management-tool` ユーティリティを使用して vCloud Director と KairosDB 間の接続を構成します。

次のようなコマンドを使用します。<KairosDB-IP> は KairosDB がインストールされたマシンの IP アドレス、または要求を KairosDB の複数のインスタンスに分配するために使用しているロード バランサーの IP アドレスです。

```
[root@cell1 /opt/vmware/vcloud-
director/bin]# ./cell-management-tool configure-metrics --repository-host
<KairosDB-IP> --repository-port 8080
```

2 `cell-management-tool` ユーティリティの `service` コマンドを使用して各 vCloud Director セルを再起動します。

インデックス

ね

ふ

ほ