

vCloud Director インストールおよびアップグレードガイド

vCloud Director 5.1

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-000749-00

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。

Copyright © 2010–2012 VMware, Inc. 無断転載を禁ず。本製品は、米国著作権法および米国知的財産法ならびに国際著作権法および国際知的財産法により保護されています。VMware 製品には、<http://www.vmware.com/go/patents-jp> に列記されている 1 つ以上の特許が適用されます。

VMware は、米国およびその他の地域における VMware, Inc. の登録商標または商標です。他のすべての名称ならびに製品についての商標は、それぞれの所有者の商標または登録商標です。

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

ヴァイエルムウェア株式会社
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	5
1 vCloud Director のインストール、構成、およびアップグレードの概要	7
vCloud Director のアーキテクチャ	7
構成の計画	8
vCloud Director のハードウェアおよびソフトウェア要件	9
2 vCloud Director Server グループの作成	23
サーバー グループの任意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	24
ネットワークおよびデータベース接続の構成	26
vCloud Director サービスの開始と停止	29
追加のサーバーへの vCloud Director ソフトウェアのインストール	30
Microsoft Sysprep デプロイ パッケージの作成	31
vCloud Director ソフトウェアのアンインストール	31
3 vCloud Director のアップグレード	33
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	35
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	43
vCloud Director データベースのアップグレード	45
vShield Manager のアップグレード	47
vCenter、ESX/ESXi ホスト、および vShield Edge アプライアンスのアップグレード	48
アップグレードされたネットワークへの変更	49
4 vCloud Director セットアップ	53
使用許諾契約書の確認	54
ライセンス キーの入力	54
システム管理者アカウントの作成	54
システム設定の指定	54
vCloud Director へのログイン準備完了	55
インデックス	57

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』では、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™ と連動できるように構成して、VMware に対応した VMware vCloud サービスを提供する方法について説明します。

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。

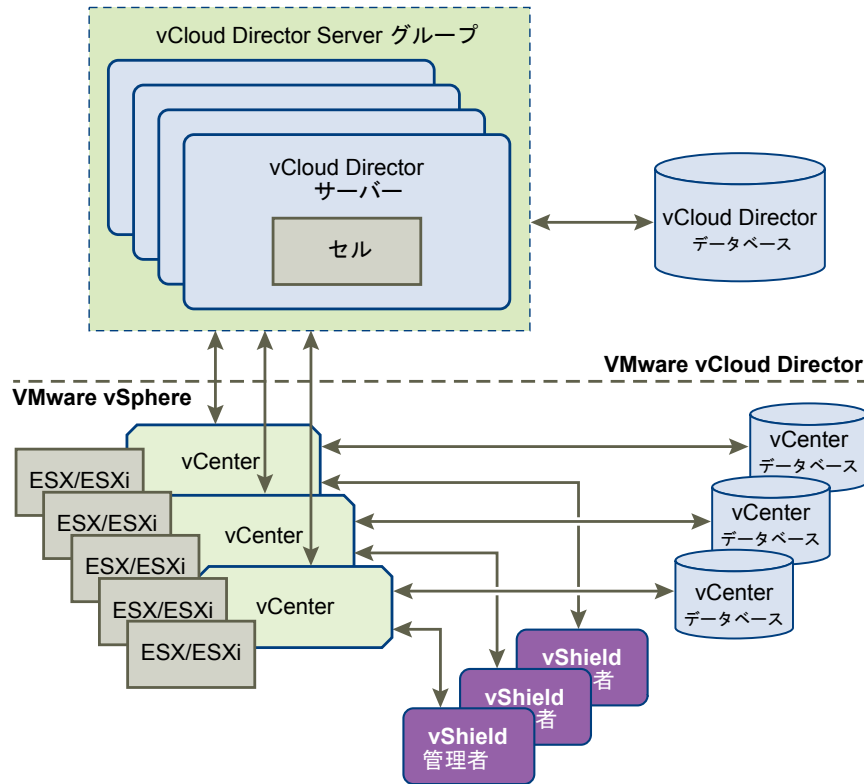
- [vCloud Director のアーキテクチャ \(P. 7\)](#)
- [構成の計画 \(P. 8\)](#)
- [vCloud Director のハードウェアおよびソフトウェア要件 \(P. 9\)](#)

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 および ESX/ESXi ホストとリンクします。vShield Manager Server は、vCenter と vCloud Director にネットワーク サービスを提供します。

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、vCenter Server が管理する ESX/ESXi ホスト、および vCenter Server をサポートするように構成されている vShield Manager サーバーに接続します。

図 1-1. 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、セルを作成して共有データベースに接続し、vCenter Server、vShield Manager、および ESX/ESXi ホストへの最初の接続を確立します。システム管理者は、vCloud Director Web コンソールを使用して、いつでも追加の vCenter Server、vShield Manager Server、および ESX/ESXi Server を vCloud Director サーバー グループに接続できます。

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 サーバーごとに 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、CPU、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 \(P. 14\)」](#) 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 Server、および 1 つ以上の ESX/ESXi ホストへのアクセス権限が必要です。

サポート対象の vCenter Server、ESX/ESXi、および vShield Manager のバージョン

サポート対象の vCenter Server、ESX/ESXi、および vShield Manager の各バージョンに関する最新情報は、「VMware Product Interoperability Matrixes」 (http://partnerweb.vmware.com/comp_guide/sim/interop_matrix.php) で確認できます。

vSphere 構成要件

vCenter Server と ESX/ESXi ホストは、vCloud Director と共に使用することが前提で、特定の構成要件を満たしている必要があります。

- 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。
- vCloud Director で使用する vCenter クラスタは、自動化 DRS を使用するように構成する必要があります。自動化 DRS は、DRS クラスタのすべてのホストに接続された共有ストレージを必要とします。
- vCenter Server は ESX/ESXi ホストを信頼する必要があります。vCloud Director によって管理されるすべてのクラスタのすべてのホストは、検証されたホスト証明書が必要とされるように構成する必要があります。特に、すべてのホストで一致するサムプリントを決定、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

Red Hat Enterprise Linux 5 (64 ビット)、Update 4

Red Hat Enterprise Linux 5 (64 ビット)、Update 5

Red Hat Enterprise Linux 5 (64 ビット)、Update 6

Red Hat Enterprise Linux 5 (64 ビット)、Update 8

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 (続き)

オペレーティング システム	
Red Hat Enterprise Linux 6 (64 ビット)、Update 1	
Red Hat Enterprise Linux 6 (64 ビット)、Update 2	

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 950MB の空き容量が必要です。
メモリ要件	各 vCloud Director サーバーに、1GB 以上のメモリをプロビジョニングする必要があります。2GB を推奨します。
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	

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。サポートされているデータベースに関する最新情報は、「VMware Product Interoperability Matrixes」(http://partnerweb.vmware.com/comp_guide/sim/interop_matrix.php) で確認できます。

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.14)」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。

vCloud Director のサポート対象ブラウザ

vCloud Director Web コンソールは、Firefox および Internet Explorer Web ブラウザの複数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。

Microsoft Windows プラットフォームのサポート対象ブラウザ

表 1-4. 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	Internet Explorer 7.<x>	Internet Explorer 8.<x>	Internet Explorer 9.<x>	Firefox 12.<x>, 13.<x>
Windows XP Professional 32 ビット	はい	はい	なし	はい
Windows XP Professional 64 ビット	はい	はい	なし	はい
Windows Server 2003 Enterprise Edition 32 ビット	はい	はい	なし	はい
Windows Server 2003 Enterprise Edition 64 ビット	はい	はい	なし	はい
Windows Server 2008	はい	はい	はい	はい
Windows Server 2008 R2	なし	はい	はい	はい
Windows Vista 32 ビット	はい	はい	はい	はい
Windows Vista 64 ビット	はい	はい	はい	はい
Windows 7 32 ビット	なし	はい	はい	はい
Windows 7 64 ビット	なし	はい	はい	はい

Linux プラットフォームでサポートされるブラウザ

表 1-5. 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	Firefox 11.<x>
Red Hat Enterprise Linux 5 (32 ビット)、Update 6	はい
Red Hat Enterprise Linux 6 (32 ビット)	はい
Red Hat Enterprise Linux 6 (64 ビット)	はい
SLES 11 32 ビット	はい
Ubuntu 10.10 32 ビット	はい
Ubuntu 10.10 64 ビット	はい

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 バージョン 10.2 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。

サポート対象の TLS および SSL プロトコルバージョンと暗号化スイート

vCloud Director では、SSL の使用にクライアントが必要です。サポート対象バージョンには、SSL 3.0 と TLS 1.0 が含まれます。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。

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 サーバー、データベース サーバ、vCenter Server、vShield Manager Server 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

vCloud Director と vShield Manager の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、`mycloud.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 mycloud
nslookup mycloud.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 `mycloud.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

アップロードとダウンロード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 クラスタ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。このボリュームには、ルートの書き込み権限が必要です。それぞれのホストは、このボリュームを `$VCLLOUD_HOME/data/transfer`、通常は `/opt/vmware/vcloud-director/data/transfer` にマウントする必要があります。アップロードとダウンロードでは、このストレージを数時間から 1 日の間占有します。大きいイメージが転送される可能性があるため、このボリュームには少なくとも数百ギガバイトを割り当てる必要があります。

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。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 사용되는 NFS ポートマッパー
920	TCP、UDP	転送サービスで 사용되는 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 사용되는 NFS ポートマッパー
123	TCP、UDP	NTP
389	TCP、UDP	LDAP
443	TCP	vCenter、vShield 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 사용되는 NFS rpc.statd
1433	TCP	デフォルトの Microsoft SQL Server データベースポート
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

- 物理ホスト コンピュータを、vCloud Director ネットワーク プールをサポートする vNetwork 分散スイッチのアプリケーションにある物理ネットワークに接続しないでください。
- 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。

データ テーブルスペース (CLOUD_DATA) とインデックス テーブルスペース (CLOUD_INDX) を別個に作成するには、次の形式のコマンドを使用します。

```
Create Tablespace CLOUD_DATA datafile '$ORACLE_HOME/oradata/cloud_data01.dbf' size 1000M autoextend on;
```

```
Create Tablespace CLOUD_INDX datafile '$ORACLE_HOME/oradata/cloud_indx01.dbf' size 500M 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 **vccloud**、パスワード **vccloudpass** を作成します。

```
Create user $vccloud identified by $vccloudpass 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/tsnames.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。

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 `tempdb` 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 `tempdb` ファイルを作成することをお勧めします。`tempdb` 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、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、データベース隔離レベルを 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離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 が必要です。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 クラスタで使用する各 vCloud Director サーバーには 2 つの SSL 証明書 (IP アドレスごとに 1 つ) が必要です。

注意 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 **vcloud.vcloud** により読み取り可能であることが必要です。このユーザーは、vCloud Director インストーラにより作成されます。

手順

- 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。
- 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>
- 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。
- 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。署名付き証明書は、最高レベルの信頼を提供します。2,048 ビットのキー長により、高レベルのセキュリティを実現します。

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 サーバーには Java キーストア ファイル内に 2 つの SSL 証明書 (IP アドレスごとに 1 つ) が必要です。vCloud Director サーバー グループ内で使用するサーバーごとに 2 つの SSL 証明書を作成する必要があります。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。署名付き証明書は、最高レベルの信頼を提供します。

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 \(P. 19\)](#)」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とそれに関連付けられた IP アドレス、各 IP アドレスに選択されたサービスのリストを生成します。「[SSL 証明書の作成 \(P. 16\)](#)」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 6 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 6 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、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。

手順

- 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。
keytool -keystore certificates.ks -storetype JCEKS -storepass <passwd> -genkey -keyalg RSA -alias http
証明書の有効期間は 90 日間です。
- keytool** の質問に答えます。
keytool から姓名を質問されたら、HTTP サービスに使用する IP アドレスに関連付けられた完全修飾ドメイン名を入力します。

- 3 残りの質問については、この例で示すように、組織と場所に該当する回答を指定します。

```

What is your first and last name? [Unknown]:mycloud.example.com
What is the name of your organizational unit?
[Unknown]:Engineering
What is the name of your organization?
[Unknown]:Example Corporation
What is the name of your City or Locality? [Unknown]:Palo Alto
What is the name of your State or Province? [Unknown]:California
What is the two-letter country code for this unit? [Unknown]:US
Is CN=mycloud.example.com, OU=Engineering, O="Example
Corporation", L="Palo Alto", ST=California, C=US correct?[no]:yes
Enter key password for <http> (RETURN if same as keystore
password):

```

- 4 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
```

- 5 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。

```
keytool -keystore certificates.ks -storetype JCEKS -storepass <passwd> -genkey -
keyalg RSA -alias consoleproxy
```

証明書の有効期間は 90 日間です。

- 6 `keytool` から姓名を質問されたら、コンソール プロキシ サービスに使用する IP アドレスに関連付けられた完全修飾ドメイン名を入力します。

- 7 残りの質問については、「[手順 3](#)」の例で示すように、組織と場所に該当する回答を指定します。

- 8 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
```

- 9 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。

- 10 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
```

- 11 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
```

- 12 残りの vCloud Director サーバーについて、それぞれ「手順 1」から「手順 11」までを繰り返します。

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 \(P. 26\)](#)」を参照してください。

注意 vCloud Director の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。

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 サーバーには Java キーストア ファイル内に 2 つの SSL 証明書 (IP アドレスごとに 1 つ) が必要です。vCloud Director サーバー グループ内で使用するサーバーごとに 2 つの SSL 証明書を作成する必要があります。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。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 \(P. 17\)](#)」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とそれに関連付けられた IP アドレス、各 IP アドレスに選択されたサービスのリストを生成します。「[SSL 証明書の作成 \(P. 16\)](#)」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 6 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 6 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、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。

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。
keytool -keystore certificates.ks -storetype JCEKS -storepass <passwd> -genkey -keyalg RSA -alias http
- 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。
keytool -keystore certificates.ks -storetype JCEKS -storepass <passwd> -genkey -keyalg RSA -alias consoleproxy
証明書の有効期間は 90 日間です。
- 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 残りの vCloud Director サーバーについて、それぞれ「[手順 1](#)」から「[手順 3](#)」までを繰り返します。

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 \(P. 26\)](#)」を参照してください。

注意 vCloud Director の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。

vShield Manager のインストールと構成

vCloud Director は、vShield Manager を利用してクラウドにネットワーク サービスを提供します。vCloud Director のインストールを開始する前に、vShield Manager をインストールして構成します。

vCloud Director に追加する各 vCenter Server を固有の vShield Manager インスタンスに関連付ける必要があります。vShield Manager のネットワーク要件とサポート対象バージョンの詳細については、「[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 の新しいインストールにのみ適用されます。vCloud Director の既存のインストールをアップグレードしている場合、関連付けられた vShield Manager インストールを任意にアップグレードすることができます。vShield Manager の新しいリリースは、既存のリリースの vCloud Director と連動することができません。「[vShield Manager のアップグレード \(P. 47\)](#)」を参照してください。

手順

- 1 vSphere Client を使用して、vCenter Server にログインします。
- 2 [ファイル] - [OVF テンプレートのデプロイ] を選択します。
- 3 **vShield Manager.ovf** ファイルの場所を参照し、案内に従って OVF ファイルをデプロイします。
- 4 OVF ファイルをデプロイしたら、vShield Manager 仮想マシンをパワーオンして、コンソールを開きます。
- 5 コンソールにユーザー名 **admin** とパスワード **default** を使用してログインします。
- 6 **manager** プロンプトで、**enable** と入力します。
- 7 **Password** プロンプトで、**default** と入力してセットアップ モードを有効にします。
セットアップ モードが有効になると、プロンプトの文字列が **manager#** に変わります。

- 8 **manager#** プロンプトで、**setup** と入力してセットアップ プロシージャを開始します。
- 9 vShield Manager 仮想マシンの IP アドレス、サブネット マスク、およびデフォルト ゲートウェイを入力します。
vCenter Server を vCloud Director に関連付けるために、この情報が必要です。
- 10 **exit** と入力してログアウトします。
- 11 コンソールを閉じ、仮想マシンは実行したままにします。
vShield Manager を vCloud Director で使用する場合、vShield Manager を vCenter と同期したり、vSphere Client プラグインとして登録したりする必要はありません。

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。

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](http://www.vmware.com) からダウンロードされた署名付きのほか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 キーを取得し、インポートします。
 - a 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。
 - b 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。
 - c 作成したディレクトリにキー ファイルを保存します。
 - d 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。

- 2 (オプション) Linux `rpm` ツールを使用して、ダウンロードされたファイルのデジタル署名を検証します。

```
# rpm --checksig <installation-file>
```

ファイルのデジタル署名を検証した後、サーバー上にパブリック キーをインストールしなくても、そのファイルを使用して vCloud Director をインストールしたり、アップグレードすることができます。インストーラは、キーがインストールされていない場合に警告します。ファイルの署名をすでに検証している場合は、警告を無視できます。

vCloud Director Server グループの作成

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。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。サーバー グループを作成するには、各サーバーに vCloud Director ソフトウェアをインストールし、ネットワークおよびデータベース接続を構成して、vCloud Director サービスを開始します。

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 \(P. 33\)\]](#) 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 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、[\[サポート対象の vCenter Server、ESX/ESXi、および vShield Manager のバージョン \(P. 9\)\]](#) を参照してください。
- 2 サポート対象の vShield Manager Server 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については、[\[サポート対象の vCenter Server、ESX/ESXi、および vShield Manager のバージョン \(P. 9\)\]](#) 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、[\[vShield Manager のインストールと構成 \(P. 20\)\]](#) を参照してください。
- 3 少なくとも 1 つのサポート対象 vCloud Director サーバー プラットフォームが実行されていて、適切な量のメモリと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 \(P. 9\)\]](#) 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 `vcloud.vcloud` により読み取り可能であることが必要です。このユーザーは、vCloud Director インストーラにより作成されます。[\[SSL 証明書の作成 \(P. 16\)\]](#) 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 `$VCLLOUD_HOME/data/transfer` (通常は `/opt/vmware/vcloud-director/data/transfer`) にマウントする必要があります。このボリュームには、ルートの書き込み権限が必要です。
 - 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 デプロイ パッケージの作成 \(P. 31\)\]](#) 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、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 \(P. 14\)」](#)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 と vShield Manager Server が互いの名前を解決できることを確認します ([「ネットワーク構成要件の要約 \(P. 12\)」](#)を参照)。
- 6 すべての vCloud Director サーバーとデータベース サーバーが、[「ネットワーク構成要件の要約 \(P. 12\)」](#)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 ファイアウォール ポートを [「ネットワーク セキュリティ要件 \(P. 13\)」](#) に示すように開きます。vCloud Director サーバーと vCenter Server 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 グループの任意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 \(P. 24\)](#)
- [ネットワークおよびデータベース接続の構成 \(P. 26\)](#)
- [vCloud Director サービスの開始と停止 \(P. 29\)](#)
- [追加のサーバーへの vCloud Director ソフトウェアのインストール \(P. 30\)](#)
- [Microsoft Sysprep デプロイ パッケージの作成 \(P. 31\)](#)
- [vCloud Director ソフトウェアのアンインストール \(P. 31\)](#)

サーバー グループの任意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 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。

vCloud Director ソフトウェアは、`vmware-vcloud-director-5.1.0-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。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。

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、[「ネットワーク構成要件の要約 \(P. 12\)」](#) 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 サーバーには、`vcloud` という名前の既存ユーザーまたはグループが存在しないようにする必要があります。
- 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。
- 複数のサーバーを含む vCloud Director サーバー グループを作成する場合、ターゲット サーバーが `$VCLLOUD_HOME/data/transfer` に共有転送サービス ストレージ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場合、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 \(P. 22\)」](#)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 チェックサムの両方の値が、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 ページのものと同じであることを確認します。以下の形式の Linux コマンドは、ダウンロード ページからコピーされた MD5 <checksum-value> を使用して <installation-file> のチェックサムを検証します。

```
md5sum -c <checksum-value>
          <installation-file>
```

- 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。

```
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 (./<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。

インストーラでは、ホストがすべての要件を満たすことを確認し、インストール ファイルのデジタル署名を検証し、vCloud Director RPM パッケージを展開して、ソフトウェアをインストールします。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
```

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。

- 6 いくつかの構成スクリプトを実行するかを決定します。

オプション	説明
すぐに構成スクリプトを実行する	y を入力して Enter を押します。
後で構成スクリプトを実行する	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\(P.26\)](#) 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メッセージが表示されますが、スクリプトは後で実行できます。vCloud Director ソフトウェアをインストールした後、別個の操作として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。

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 \(P. 14\)\]](#) 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 \(P. 17\)\]](#) 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 \(P. 14\)\]](#) 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 \(P. 14\)\]](#) 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、[追加のサーバーへのvCloud Directorソフトウェアのインストール\(P.30\)](#) 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 \(P. 53\)\]](#) 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。

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。この例に示すように、ファイルの所有者は必ず **vcloud.vcloud** にし、所有者の読み取り/書き込み権限を設定する必要があります。設定されていないと、構成スクリプトが応答ファイルを使用できません。

```
% ls -l responses.properties
-rw----- 1 vcloud vcloud 418 Jun 8 13:42
responses.properties
```

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。

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 \(P. 35\)」](#) 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。 <code>service vmware-vcd start</code>
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。 <code>service vmware-vcd stop</code>

追加のサーバーへの 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。同じサーバー グループのすべてのサーバーに、同じデータベース接続の詳細を構成する必要があります。この要件を確実に満たすためには、最初のサーバー インストールで作成された応答ファイルを使用して、追加のサーバーのインストール時にこの情報を指定します。

開始する前に

このインストール環境に最初のサーバーをインストールしたときに作成された応答ファイルのコピーは、グループに追加するすべてのサーバーからアクセスできる必要があります。[「応答ファイルの保護と再利用 \(P.29\)」](#) 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 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。

```
chmod u+x <installation-file>
```

- 4 インストール ファイルを実行し、応答ファイルのパス名を指定します。

インストールのコマンドラインに `-r` オプションを指定し、そのオプションの引数として応答ファイルのフルパス名を指定します。

```
<installation-file> -r <path-to-response-file>
```

- 5 (オプション) この手順をこのインストール環境に追加するすべてのサーバーについて繰り返します。

インストーラでは、ネットワーク接続情報が要求され、応答ファイルの応答を使用してネットワークおよびデータベース接続がセットアップされます。

次に進む前に

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 \(P. 53\)\]](#) を参照してください。

Microsoft Sysprep デプロイ パッケージの作成

vCloud Director が特定の 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、インストール環境のクラウドセルごとに Microsoft Sysprep デプロイメント パッケージを作成しておく必要があります。

vCloud Director のインストール時に、vCloud Director サーバホストの **sysprep** フォルダに複数のファイルが配置されます。Sysprep パッケージを作成するときにこれらのファイルを上書きしないでください。

開始する前に

Windows 2000、Windows 2003 (32 ビットおよび 64 ビット)、Windows XP (32 ビットおよび 64 ビット) の Sysprep バイナリ ファイルへのアクセス。

手順

- 1 各オペレーティングシステムの Sysprep バイナリ ファイルを、vCloud Director サーバホスト上の任意の場所にコピーします。

オペレーティングシステムごとに独自のフォルダが必要です。

注意 フォルダ名では大文字と小文字が区別されます。

ゲスト OS	コピー先
Windows 2000	<SysprepBinariesDirectory> /win2000
Windows 2003 (32 ビット)	<SysprepBinariesDirectory> /win2k3
Windows 2003 (64 ビット)	<SysprepBinariesDirectory> /win2k3_64
Windows XP (32 ビット)	<SysprepBinariesDirectory> /winxp
Windows XP (64 ビット)	<SysprepBinariesDirectory> /winxp_64

<SysprepBinariesDirectory> は、バイナリのコピー先として選択した場所を表します。

- 2 `/opt/vmware/vcloud-director/deploymentPackageCreator/createSysprepPackage.sh` <SysprepBinariesDirectory> コマンドを実行します。
たとえば、`/opt/vmware/vcloud-director/deploymentPackageCreator/createSysprepPackage.sh /root/MySysprepFiles` です。
- 3 クラウドセルを再起動するには、`service vmware-vcd restart` コマンドを実行します。
- 4 複数のクラウドセルがある場合、パッケージとプロパティ ファイルをすべてのクラウドセルにコピーします。

```
scp /opt/vmware/vcloud-director/guestcustomization/vcloud_sysprep.properties /opt/vmware/vcloud-director/guestcustomization/windows_deployment_package_sysprep.cab root@<next_cell_IP>:/opt/vmware/vcloud-director/guestcustomization
```
- 5 ファイルのコピー先の各クラウドセルを再起動します。

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

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。vShield Manager、vCenter、ESX/ESXi を含め、vCloud Director をサポートする vSphere コンポーネントをアップグレードする必要もあります。

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。

重要 アップグレード プロセスでは、vCloud Director、vShield Manager、vCenter および ESX/ESXi のアップグレードが必要です。vShield Manager のアップグレード手順が完了する前にユーザーが vCloud Director へアクセスしないようにしてください。

アップグレードでは、次の成果物が保存されます。

- 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。

クラウドでロード バランサーを使用している場合、サーバー グループのサブセットはアップグレードし、それ以外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。ロード バランサーがない場合、アップグレードの際には、データベースと少なくとも 1 つのサーバーをアップグレードするのに十分な vCloud Director ダウンタイムが必要になります。また、登録された vCenter Server で互換性のあるバージョンの vCenter ソフトウェアが実行されていない場合には、それらの vCenter Server をアップグレードする必要もあります。ホストまたは vCenter Server のアップグレード中はそれらの仮想マシンにアクセスできなくなるため、vCenter Server または ESX/ESXi ホストのアップグレードによって vCloud Director のダウンタイムが長くなる可能性があります。

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 \(P. 35\)」](#) 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\(P.39\)」](#) 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 \(P. 29\)\]](#) を参照してください。
- 6 vShield Manager を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 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 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 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 の本リリースで導入されたネットワーク機能を使用するには、[\[サポート対象の vCenter Server、ESX/ESXi、および vShield Manager のバージョン \(P. 9\)\]](#) に一覧表示されている vShield Manager の最新バージョンが必要です。 [\[vShield Manager のアップグレード \(P. 47\)\]](#) を参照してください。
- 7 ユーザーの vCloud Director へのアクセスを再度有効化します。
- 8 vCenter と ESX/ESXi ホストをアップグレードします。 [\[vCenter、ESX/ESXi 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 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 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 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。 [\[サポート対象の vCenter Server、ESX/ESXi、および vShield Manager のバージョン \(P. 9\)\]](#) を参照してください。
- 9 アップグレードされたネットワーク内の変更を確認し、必要に応じてファイアウォールルールを再構成します。 [\[アップグレードされたネットワークへの変更 \(P. 49\)\]](#) を参照してください。

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。

- 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。 [\[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 \(P. 35\)\]](#) 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 \(P. 29\)\]](#) を参照してください。
- 7 vShield Manager をアップグレードします。 [\[vShield Manager のアップグレード \(P. 47\)\]](#) を参照してください。
- 8 vCenter と ESX/ESXi ホストをアップグレードします。 [\[vCenter、ESX/ESXi 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。
- 11 アップグレードされたネットワーク内の変更を確認し、必要に応じてファイアウォールルールを再構成します。 [\[アップグレードされたネットワークへの変更 \(P. 49\)\]](#) 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。そのセルのメンテナンス メッセージをオンにするには、セルで `/opt/vmware/vcloud-director/bin/vmware-vcd-cell` コマンドを実行します。

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

このコマンドは、アップグレードの前後に 1 つのセルで実行できます。セルのアップグレード準備ができたか、アップグレードされたセルをサービスに戻す場合は、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]#
./vmware-vcd-cell stop
```

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 \(P. 35\)](#)
- [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 \(P. 43\)](#)
- [vCloud Director データベースのアップグレード \(P. 45\)](#)
- [vShield Manager のアップグレード \(P. 47\)](#)
- [vCenter、ESX/ESXi ホスト、および vShield Edge アプライアンスのアップグレード \(P. 48\)](#)
- [アップグレードされたネットワークへの変更 \(P. 49\)](#)

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。[「セル管理ツール リファレンス \(P. 36\)」](#) 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。

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 -p
Pa55w0rd 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 -p
Pa55w0rd 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 -p
Pa55w0rd cell --shutdown
```

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できます。

セル管理ツール リファレンス

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
-p,--password <arg> administrator password
-u,--username <arg> administrator username
```

Available commands:

```
cell - Manipulates the Cell and core components
```

dbextract – Exports the data from the given set of tables
certificates – Reconfigures the SSL certificates for the cell
generate-certs – Generates self-signed SSL certificates for use with vCD cell
recover-password – Change a forgotten System Administrator password. Database credentials are required

For command specific help:

cell-management-tool [...] <commandName> -h

- [セルを管理するためのコマンド \(P. 37\)](#)
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 テーブルをエクスポートするためのコマンド \(P. 38\)](#)
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。
- [SSL 証明書を置換するためのコマンド \(P. 40\)](#)
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。
- [自己署名付き SSL 証明書を生成するためのコマンド \(P. 41\)](#)
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。
- [システム管理者のパスワードの復元 \(P. 42\)](#)
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。

セルを管理するためのコマンド

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。

<command> cell サブコマンド。

表 3-1. 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。
--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	セルで実行中のジョブの数とセルのステータスに関する情報を表示します。

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、実行中のジョブ数を返します。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 -p Pa55w0rd cell --status
      Job count = 3
Is Active = true
```

データベース テーブルをエクスポートするためのコマンド

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 3-2. 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
<code>--help (-h)</code>	なし	このカテゴリで使用可能なコマンドの概要を示します。
<code>-categories</code>	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。
<code>-dataFile</code>	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 <code>\$VCLLOUD_HOME/etc/data_to_export.properties</code> を使用します。「エクスポートするテーブルと列の指定 (P. 39)」を参照してください。
<code>-dumpFile</code>	ダンプ ファイルへの絶対パス。	すべてのデータがこのファイルにエクスポートされます。
<code>-exportSettingsFile</code>	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 <code>\$VCLLOUD_HOME/etc/vCloud_0LH_JP.ini</code> を使用します。「エクスポートする行の制限と順序 (P. 40)」を参照してください。
<code>-properties</code>	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、 <code>\$VCLLOUD_HOME/etc/global.properties</code> のデータベース接続プロパティを使用します。「プロパティ ファイルの指定 (P. 39)」を参照してください。
<code>-tables</code>	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 `$VCLLOUD_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。
<パスワード>	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、 <code>orcl.example.com</code> 。
<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 `$VCLLOUD_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 `vCloud_OLH_JP.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。

この例の `vCloud_OLH_JP.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 `$VCLLOUD_HOME/etc/vCloud_OLH_JP.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 -dumpFile /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.
```

SSL 証明書を置換するためのコマンド

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 \(P. 17\)」](#) 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 3-3. セル管理ツールのオプションと引数、`certificates` サブコマンド

オプション	引数	説明
<code>--help (-h)</code>	なし	このカテゴリで使用可能なコマンドの概要を示します。
<code>--config (-c)</code>	セルの <code>global.properties</code> ファイルへのフルパス名	デフォルトで <code>\$VCLLOUD_HOME/etc/global.properties</code> です。
<code>--responses (-r)</code>	セルの <code>responses.properties</code> ファイルへのフルパス名	デフォルトで <code>\$VCLLOUD_HOME/etc/responses.properties</code> です。
<code>--keystore (-s)</code>	<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。
<code>--keystore-pwd (-w)</code>	<keystore-password>	<code>--keystore</code> オプションによって参照される JCEKS キーストアのパスワードです。

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/new.ke` に存在し、パスワードは `kspw` となっています。この例では、セルの既存の証明書が `/tmp/new.ke` に存在する証明書で置換されます。

```
[root@cell1 /opt/vmware/vcloud-director/bin]#
./cell-management-tool certificates -s /tmp/my-new-certs.ke -w kspw
Certificate replaced by user specified keystore at /tmp/new.ke.
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。

自己署名付き SSL 証明書を生成するためのコマンド

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 \(P. 19\)](#)」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 3-4. 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
<code>--help (-h)</code>	なし	このカテゴリで使用可能なコマンドの概要を示します。
<code>-issuer (-i)</code>	<name>=<value> [, <name>=<value>, ...]	証明書発行者の X.509 識別名。デフォルトでは <code>CN=Unknown</code> 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ってください。
<code>--out (-o)</code>	<keystore-pathname>	このホスト上のキーストアへのフルパス名です。

表 3-4. セル管理ツールのオプションと引数、generate-certs サブコマンド (続き)

オプション	引数	説明
--key-size (-s)	<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 1024 です。
--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。
--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。

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、パスワードを `kspw` と想定しています。このキーストアは、まだ存在しない場合には作成されます。

この例では、デフォルト値を使用して新しい証明書を作成します。発行者名は `CN=Unknown` に設定されています。証明書では、1024 ビットの暗号化が使用されており、これは作成の 1 年後に有効期限切れとなります。

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

この例では、キー サイズと発行者名にカスタム値を使用して新しい証明書を作成します。発行者名は `CN=Test, L=London, C=GB` に設定されています。証明書では、2048 ビットの暗号化が使用されており、これは作成の 90 日後に有効期限切れとなります。

```
[root@cell1 /opt/vmware/vcloud-director/bin]#
      ./cell-management-tool generate-certs -o /tmp/cell.ks -w kspw
      -i "CN=Test, L=London, C=GB" -s 2048 -x 90
New keystore created and written to /tmp/cell.ks.
```

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 3-5. 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。

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-5.1.0-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

- 組織ネットワークを含むシステム内のすべての組織が、組織 vDC も含んでいることを確認します。アップグレードプロセスにより既存の組織ネットワークが組織 vDC ネットワークに変換されるため、組織ネットワークを含んでいても、組織 vDC を含んでいない組織はアップグレードすることができず、データベースのアップグレードが失敗します。
- 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。
- インストーラにインストール ファイルのデジタル署名を検証させる場合、ターゲットサーバーに 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. 22)] 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。

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 チェックサムの両方の値が、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。以下の形式の Linux コマンドは、ダウンロード ページからコピーされた MD5 <checksum-value> を使用して <installation-file> のチェックサムを検証します。

```
md5sum -c <checksum-value>
                <installation-file>
```
- 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。

```
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. 35)] 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、このサーバーをアップグレードするかどうか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. Would you like
to upgrade it? The installer will stop the vmware-vcd service,
back up any configuration files from the previous release and migrate the
product configuration as necessary.
```

- 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。

```
Would you like to upgrade now? (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
```

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、次の警告を表示します。

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

- 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 <code>/opt/vmware/vcloud-director/etc/log4j.properties</code> にコピーします。
ログ記録プロパティを変更した場合	<code>/opt/vmware/vcloud-director/etc/log4j.properties.rpmnew</code> ファイルを既存の <code>/opt/vmware/vcloud-director/etc/log4j.properties</code> 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 \(P. 29\)](#)] 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。

- データベースを使用している vCloud Director サーバーが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 \(P. 35\)](#)] 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 データベース アップグレード スクリプトが互換性のない vShield Manager のバージョンが vCloud Director のこのインストールに登録されているのを検出した場合、この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 to vShield Manager version 5.0 or later versions.
```

[[vShield Manager のアップグレード \(P. 47\)](#)] を参照してください。

- 2 データベース アップグレード プロンプトに回答します。

Welcome to the vCloud Director upgrade utility

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]:

y

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。

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。

```
Examining database at URL: jdbc:oracle:thin:@10.26.50.54:1521/orcl
Applying 1 upgrade batches
Executing upgrade batch:
Executing SQL statements from file: cc-tool-uninstall-graceful.sql
.....
Executing SQL statements from file: Upgrade.sql []
.....
Executing SQL statements from file: Upgrade_Data.sql []
.....
Executing SQL statements from file: NewInstall_Indexes.sql []
.....
Executing SQL statements from file: Upgrade_UUID.sql []
.....
Executing SQL statements from file: NewInstall_Funcs.sql []
.....

Successfully applied upgrade batch:
Running 2 upgrade tasks
Successfully ran upgrade task
Successfully ran upgrade task
Applying 1 upgrade batches
Executing upgrade batch: cleanup
Executing SQL statements from file: NewInstall_Funcs.sql []
.....
Executing SQL statements from file: Upgrade_UUID_Clean.sql []
.....
Executing SQL statements from file: Upgrade_Clean.sql []
.....

Successfully applied upgrade batch: cleanup
Database upgrade complete
+++++
```

- 3 (オプション) データベース インデックスを再構築し、データベースの統計情報を更新します。

これらの手順はオプションであり、アップグレード後のデータベースのパフォーマンス向上につながる可能性があります。

Do you wish to rebuild the database indexes? This may take several minutes. [Y/N]

y

Rebuilding database indexes

...

Do you wish to update the database statistics? This may take several minutes. [Y/N]

y

Updating database statistics

...

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).
```

vShield Manager のアップグレード

vCloud Director に登録された vCenter および ESX/ESXi ホストをアップグレードする前に、vCenter Server に接続された vShield Manager サーバをアップグレードする必要があります。

vCloud Director に接続された vCenter Server をアップグレードする前に、アップグレードされた vCenter Server に関連付けられた vShield Manager サーバをアップグレードしてください。vShield Manager のアップグレードは、vShield Manager 管理機能へのアクセスを中断しますが、ネットワーク サービスは中断しません。

開始する前に

vCloud Director のインストールで少なくとも 1 つのアップグレードされたセルが、このアップグレードが始まる前に実行中でなければなりません。このセルはアップグレードされた vShield Manager についてのデータを vCloud Director データベースに書き込む責任を持っています。

手順

- 1 vShield Manager をアップグレードします。

『vShield クイック スタート ガイド』の手順に従ってください。アップグレードが完了した後で、vShield Manager は vCloud Director に対して、新しいバージョンが利用できることを通知します。vShield Manager が通知を送り、vCloud Director がそれを処理するまでに数分かかることがあります。

- 2 vShield Manager をアップグレードした後で、アップグレードされた vShield Manager が管理する vShield Edge アプライアンスをアップグレードする前に、すべての vCenter と ESX/ESXi ホストをアップグレードする必要があります。

vCenter、ESX/ESXi 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 をアップグレードした後で、クラウドに接続された vCenter Server および ESX/ESXi ホストをアップグレードして、その後、アップグレードされた vCenter Server 上で vShield Edge アプライアンスをアップグレードします。

手順

- 1 vCenter Server 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 vCloud Director での vCenter Server 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。
- 3 アップグレードされた vCenter Server がサポートするそれぞれの ESX/ESXi 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 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の別のホストへの移行を許可します。
 - 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 を使用してホストと再接続します。
 - 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 を使用してホストのメンテナンス モードを終了します。
- 4 アップグレードされた vCenter Server 上の vShield Manager が管理するすべての vShield Edge アプライアンスをアップグレードしてください。
このアップグレードを管理するために、vShield Manager ユーザー インターフェイスを使用します。

注意 vCloud Director Web コンソールまたは REST API を使用して、vShield Edge が保護するネットワークをリセットする場合、このアップグレードは自動的に行われます。vShield Manager ユーザー インターフェイスを使用して vShield Edge を管理すると、アップグレード プロセスと関連のネットワーク ダウンタイムをより良く管理できます。

アップグレードされたネットワークへの変更

vCloud Director ネットワーク インフラストラクチャにおける変更により、場合によっては、アップグレード プロセスによって既存のネットワークおよびサービスが変更されることがあります。これらの変更はいずれも、既存のネットワーク接続に影響するものではありませんが、一部のネットワーク サービスにはアップグレード後の再構成が必要となる場合があります。

組織ネットワーク

vCloud Director を今回のリリースにアップグレードするとき、既存の組織ネットワークは新しい vCloud Director のネットワーク インフラを使用するよう変換されます。アップグレードされた組織ネットワークでは、次の変更が見られると考えられます。

- 経路指定されている組織ネットワークが、経路指定されている組織 vDC ネットワークになります。これらのネットワークは、1 つの組織 vDC 中の Edge ゲートウェイへ接続されます。NAT やファイアウォールなど、組織ネットワーク内で定義されていたサービスが Edge ゲートウェイ内で定義されるようになります。組織に複数の vDC がある場合、アップグレード中に作成された組織 vDC ネットワークは、組織内のすべての vDC に共有されます。
- 隔離された組織ネットワークは、隔離された組織 vDC ネットワークになります。
- 直接接続されているネットワークは変更されません。
- 新しい組織 vDC ネットワークは、ネットワークが作成される組織 vDC に割り当てられるネットワーク プールを使用します。
- 経路指定されている組織ネットワーク内の NAT ルールが Edge ゲートウェイの NAT ルールに変換されます。それぞれのルールの表現方法は異なっても、その効果は変わりません。NAT ルールの詳細については、『vCloud Director 管理者ガイド』を参照してください。経路指定されている vApp ネットワーク内の NAT ルールは変更されません。

Edge ゲートウェイおよび vApp ネットワーク

ファイアウォール サービスおよびファイアウォール ルールが変更され、Edge ゲートウェイと vApp ネットワークの両方で構成の柔軟性が高まりました。

アップグレード後、Edge ゲートウェイおよび経路指定された vApp ネットワーク内のすべてのファイアウォール サービスは互換性モードで動作します。これにより、ファイアウォール ルールの操作的意味論が維持されます。既存のファイアウォール ルールを現在の形式に変換した後、ネットワークをアップグレードし、互換性モードによる制限を解除できます。ファイアウォール ルールの詳細については、『vCloud Director 管理者ガイド』を参照してください。

互換性モードでのネットワークの制限

システムが互換性モードの場合は、いくつかの制限がかけられます。

- それぞれの Edge ゲートウェイがサポートできるのは、1 つのアップリンクと 1 つの内部インターフェイスとなります。このため、1 つの Edge ゲートウェイにつき 1 つの経路指定された組織 vDC ネットワークのみが存在することになります。
- バージョン 5.1 のファイアウォール ルールをファイアウォール サービス内で作成することができません。

これらの制限を解除するには、[「Edge ゲートウェイおよび vApp ネットワークの通常の操作を有効化するための再構成 \(P. 50\)」](#) を参照してください

Edge ゲートウェイおよび vApp ネットワークの通常の操作を有効化するための再構成

既存のファイアウォール ルールを現在の形式に変換した後、Edge ゲートウェイおよび vApp ネットワークを再構成し、通常の操作を有効化して互換性モードによる制限を解除できます。

vCloud Director のこれまでのリリースでは、ファイアウォール ルールはそのルールの対象となるパケットの方向を指定していました。今回のリリースから、パケットの方向はソースおよびターゲットの IP アドレスに由来するようになっていきます。ファイアウォール ルールの [ソース] または [ターゲット] IP アドレスにおいて、**any** というキーワードまたは IP アドレスのほか、**internal** および **external** というキーワードを使用できるようになりました。

アップグレード後、Edge ゲートウェイおよび vApp ネットワーク内のすべてのファイアウォール サービスは互換性モードで動作します。これにより、ファイアウォール ルールの操作的意味論が維持されます。既存のファイアウォール ルールを現在の形式に変換した後、ネットワークをアップグレードし、互換性モードによる制限を解除できます。ファイアウォール ルールの詳細については、『vCloud Director 管理者ガイド』を参照してください。

手順

- 1 すべての Edge ゲートウェイを再デプロイします。
 - それぞれの Edge ゲートウェイを右クリックし、[再デプロイ] を選択します。
- 2 すべての vApp ネットワークを再デプロイします。
 - それぞれの vApp ネットワークを右クリックし、[ネットワークをリセット] を選択します。
- 3 すべての Edge ゲートウェイのファイアウォール ルールを現在の形式に変換します。
 - [ゲートウェイ サービス] ページの [ファイアウォール] タブの [ルールの変換] をクリックすると、ルールを自動的に変換できます。ルールを手動で変換することもできます。
 - a [ゲートウェイ サービス] ページの [ファイアウォール] タブで、ルールを選択し、[編集] をクリックします。
 - b [変換された IP 上のルールに一致] チェック ボックスをオフにします。
 - c **any** を使用して [ソース] または [ターゲット] の IP アドレスを指定する場合は必ず、**internal** または **external** を代わりに使用します。
 - d ルールがターゲット NAT の提供を意図するものである場合、[ターゲット] IP アドレスを **internal** から **external** へ変更します。
- 4 すべての vApp ネットワークのファイアウォール ルールを現在の形式に変換します。
 - vApp ネットワークの [サービスの構成] ページの [ファイアウォール] タブの [ルールの変換] をクリックすると、ルールを自動的に変換できます。ルールを手動で変換することもできます。
 - a vApp ネットワークの [サービスの構成] ページの [ファイアウォール] タブで、ルールを選択し、[編集] をクリックします。
 - b [変換された IP 上のルールに一致] チェック ボックスをオフにします。
 - c **any** を使用して [ソース] または [ターゲット] の IP アドレスを指定する場合は必ず、**internal** または **external** を代わりに使用します。
 - d ルールがターゲット NAT の提供を意図するものである場合、[ターゲット] IP アドレスを **internal** から **external** へ変更します。
- 5 すべての Edge ゲートウェイを再構成し、互換性モードの制約を解除します。
 - [Edge ゲートウェイのプロパティ] ページの [全般] タブで、[複数インターフェイス サポートを有効化] を選択します。

- 6 すべての vApp ネットワークを再構成し、互換性モードの制約を解除します。
 - a [マイクラウド] タブをクリックし、左側のペインで [vApp] をクリックします。
 - b vApp を右クリックし、[開く] を選択します。
 - c [ネットワーク] タブで、[ネットワークの詳細を表示] を選択します。
 - d vApp ネットワークを右クリックし、[サービスの構成] を選択します。
 - e [ファイアウォール] タブで、[元のアドレス上のルールのみ的一致] を選択します。

vCloud Director セットアップ

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はセットアップ 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。
- 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 \(P. 54\)](#)
- [ライセンス キーの入力 \(P. 54\)](#)
- [システム管理者アカウントの作成 \(P. 54\)](#)
- [システム設定の指定 \(P. 54\)](#)
- [vCloud Director へのログイン準備完了 \(P. 55\)](#)

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 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 vCenter 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 [システム名] フィールドに vCloud Director vCenter 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的インストール 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

vCenter と vShield Manager へのアクセス権があることを確認します。vCloud Director Web コンソールには、vCloud Director の一部として構成する vCenter と vShield Manager のインストール環境へのアクセス権が必要で、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。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 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。

インデックス

A

AMQP ブローカー、インストールおよび構成 21

E

ESX/ESXi、アップグレード 48

J

Java、必要な JRE バージョン 11

M

Microsoft Sysprep 31

R

RPM ファイル、デジタル署名を検証する 22

V

vCenter

アップグレード 48

サポート対象のリリース 9

vShield Manager

アップグレード 47

インストールと構成 20

サポート対象のリリース 9

あ

アップグレード

最初のサーバー 43

データベース 45

ワークフロー 33

い

インストール ID、指定 54

インストール

アーキテクチャ図 7

アンインストール 31

概要 7

キャパシティ プランニング 8

構成 53

最初のサーバー 24

作成 23

追加サーバー 30

お

応答ファイル

権限と所有権 29

セキュリティ 29

き

キーストア 16

け

ゲストのカスタマイズ、準備 31

こ

構成、設定の確認と完了 55

互換性モード、アップグレード 50

さ

サービス、開始 29

し

システム管理者アカウント

作成 54

パスワードの復元 42

システム名、指定 54

使用許諾契約書 54

証明書

自己署名付き 19

署名付き 17

せ

製品シリアル番号

入力 54

利用 54

セキュリティ、応答ファイル 29

セル管理ツール

cell コマンド 37

certificates コマンド 40

dbextract コマンド 38

generate-certs コマンド 41

オプション 36

て

データベース

Oracle 14

SQL Server 15

アップグレード 45

サポート対象プラットフォーム 9

接続の詳細 26

説明 14

ね

ネットワーク

アップグレード済み 49

構成要件 12

セキュリティ 13

ふ

ファイアウォール、ポートとプロトコル 13

ブラウザ、サポート対象 11