

# vCloud Director 安裝、設定 與升級指南

2019 年 3 月 28 日

VMware Cloud Director 9.7

您可以在 VMware 網站上找到最新的技術文件，網址如下：

<https://docs.vmware.com/tw/>

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

Copyright © 2010-2020 VMware, Inc. 保留所有權利。 [版權與商標資訊](#)。

# 目錄

- vCloud Director 安裝、設定與升級指南 6
- 更新資訊 7
- 1 vCloud Director 安裝、組態及升級的概觀 8**
  - vCloud Director 架構 8
  - 組態規劃 9
- 2 vCloud Director 硬體及軟體需求 10**
  - vCloud Director 的網路組態需求 11
  - 網路安全性需求 12
- 3 安裝 vCloud Director 或部署 vCloud Director 應用裝置之前 14**
  - 準備 vCloud Director 資料庫 14
    - 在 Linux 上設定 vCloud Director 的外部 PostgreSQL 資料庫 14
    - 設定 Linux 版 vCloud Director 的外部 Microsoft SQL Server 資料庫 15
  - 準備傳輸伺服器儲存區 17
  - 下載並安裝 VMware 公用金鑰 19
  - 為 vCloud Director 安裝和設定 NSX Data Center for vSphere 20
  - 為 vCloud Director 安裝和設定 NSX-T Data Center 20
- 4 針對 Linux 上的 vCloud Director 建立和管理 SSL 憑證 22**
  - 為 Linux 上的 vCloud Director 建立 SSL 憑證之前 22
  - 為 Linux 上的 vCloud Director 建立自我簽署的 SSL 憑證 23
  - 為 Linux 上的 vCloud Director 建立 CA 簽署的 SSL 憑證金鑰儲存區 24
  - 為 Linux 上的 vCloud Director 建立包含已匯入私密金鑰的 CA 簽署的 SSL 憑證金鑰儲存區 26
- 5 在 Linux 上安裝 vCloud Director 29**
  - 在伺服器群組的第一個成員上安裝 vCloud Director 軟體 30
  - 設定網路與資料庫連線 32
    - 互動式組態參考 33
    - 自動組態參考 34
    - 保護和重複使用回應檔 37
  - 在伺服器群組的其他成員上安裝 vCloud Director 37
  - 設定 vCloud Director 39
- 6 部署 vCloud Director 應用裝置 41**

- 應用裝置部署和資料庫高可用性組態 42
- 部署 vCloud Director 應用裝置的必要條件 45
- 使用 vSphere Web Client 或 vSphere Client 部署 vCloud Director 應用裝置 45
  - 啟動 vCloud Director 應用裝置部署 46
  - 自訂 vCloud Director 應用裝置並完成部署 47
- 使用 VMware OVF Tool 部署 vCloud Director 應用裝置 49
  
- 7 vCloud Director 應用裝置 SSL 憑證建立和管理 55**
  - 使用已簽署的萬用字元憑證部署 vCloud Director 應用裝置以進行 HTTPS 和主控台 Proxy 通訊 55
  - 建立 CA 簽署的 SSL 憑證並將其匯入至 vCloud Director 應用裝置 57
  - 將私密金鑰和 CA 簽署的 SSL 憑證匯入至 vCloud Director 應用裝置 59
  - 取代自我簽署的內嵌式 PostgreSQL 和 vCloud Director 應用裝置管理 UI 憑證 61
  - 更新 vCloud Director 應用裝置憑證 62
  
- 8 vCloud Director 應用裝置組態 64**
  - 檢視資料庫高可用性叢集中的儲存格的狀態 64
  - 從高可用性叢集中的主要資料庫故障復原 65
  - vCloud Director 應用裝置的內嵌式資料庫備份和還原 66
    - 備份 vCloud Director 應用裝置的內嵌式資料庫 66
    - 還原具有高可用性資料庫組態的 vCloud Director 應用裝置環境 66
    - 還原不具有高可用性資料庫組態的 vCloud Director 應用裝置環境 69
  - 設定 vCloud Director 資料庫的外部存取權 71
  - 啟用或停用對 vCloud Director 應用裝置的 SSH 存取 72
  - 編輯 vCloud Director 應用裝置的 DNS 設定 73
  - 編輯 vCloud Director 應用裝置網路介面的靜態路由 73
  - vCloud Director 應用裝置中的組態指令碼 74
  - 在 vCloud Director 應用裝置中修改 PostgreSQL 組態 74
  
- 9 在高可用性叢集組態中使用 Replication Manager 工具套件 76**
  - 檢查資料庫高可用性叢集的連線狀態 76
  - 檢查資料庫高可用性叢集中節點的複寫狀態 77
  - 檢查資料庫高可用性叢集的狀態 78
  - 偵測高可用性叢集中恢復連線的前主要節點 79
  - 在資料庫高可用性叢集中切換主要儲存格和待命儲存格的角色 81
  - 解除登錄資料庫高可用性叢集中失敗或無法連線的待命節點 82
  - 解除登錄資料庫高可用性叢集中失敗的主要儲存格 83
  - 解除登錄資料庫高可用性叢集中正在執行的待命儲存格 83
  
- 10 安裝 vCloud Director 或部署 vCloud Director 應用裝置之後 85**
  - 在伺服器上安裝 Microsoft Sysprep 檔案 85
  - 自訂公用端點 86

- 安裝和設定 RabbitMQ AMQP Broker 88
- 安裝並設定 Cassandra 資料庫以儲存歷史度量資料 89
- 在外部 PostgreSQL 資料庫上執行其他組態 90
  
- 11 升級 vCloud Director 和修補 vCloud Director 應用裝置 92**
  - 對 vCloud Director 安裝進行有組織地升級 94
  - 手動升級 vCloud Director 安裝 96
    - 升級 vCloud Director 儲存格 97
    - 升級 vCloud Director 資料庫 99
  - 資料庫升級公用程式參考 100
  - 修補 vCloud Director 應用裝置部署 101
  
- 12 移轉至 vCloud Director 應用裝置 104**
  - 將使用外部 Microsoft SQL 資料庫的 vCloud Director 移轉到 vCloud Director 應用裝置 104
  - 將使用外部 PostgreSQL 資料庫的 vCloud Director 移轉到 vCloud Director 應用裝置 107
  
- 13 升級或移轉 vCloud Director 之後 112**
  - 升級與已連接 vCenter Server 系統相關聯的每個 NSX Manager 112
  - 升級 vCenter Server 系統、ESXi 主機和 NSX Edge 112
  - 此版本中的新權限 114
  
- 14 疑難排解 vCloud Director 應用裝置 116**
  - 檢查 vCloud Director 應用裝置中的記錄檔 116
  - vCloud Director 儲存格在應用裝置部署後無法啟動 117
  - 移轉或還原到 vCloud Director 應用裝置時重新設定 vCloud Director 服務失敗 117
  - 使用記錄檔對 vCloud Director 更新和修補程式進行疑難排解 117
  - 檢查 vCloud Director 更新失敗 118
  - 安裝 vCloud Director 的最新更新失敗 118
  
- 15 解除安裝 vCloud Director 軟體 120**

# vCloud Director 安裝、設定與升級指南

《vCloud Director 安裝、設定與升級指南》提供安裝和升級 VMware vCloud Director<sup>®</sup> for Service Providers 軟體以及將其設定為與 VMware vSphere<sup>®</sup>、VMware NSX<sup>®</sup> for vSphere<sup>®</sup> 和 VMware NSX-T<sup>™</sup> Data Center 搭配使用的相關資訊。

## 主要對象

《vCloud Director 安裝、設定與升級指南》適用於想要安裝或升級 vCloud Director 軟體的任何人。本手冊中的資訊是針對熟悉 Linux、Windows、IP 網路和 vSphere 的資深系統管理員所撰寫。

# 更新資訊

本《vCloud Director 安裝、設定與升級指南》隨產品的每個版本更新或在必要時進行更新。

下表提供了《vCloud Director 安裝、設定與升級指南》的更新歷程記錄。

修訂版	描述
2019 年 6 月 11 日	<ul style="list-style-type: none"><li>■ 新增了<a href="#">更新 vCloud Director 應用裝置憑證</a>主題。</li><li>■ 新增了<a href="#">第 9 章 在高可用性叢集組態中使用 Replication Manager 工具套件</a>章節。</li></ul>
2019 年 5 月 10 日	<ul style="list-style-type: none"><li>■ 新增了<a href="#">#unique_5</a> 章節。</li><li>■ 新增了<a href="#">使用記錄檔對 vCloud Director 更新和修補程式進行疑難排解</a>主題。</li><li>■ 新增了<a href="#">檢查 vCloud Director 更新失敗</a>主題。</li><li>■ 新增了<a href="#">安裝 vCloud Director 的最新更新失敗</a>主題。</li></ul>
2019 年 4 月 05 日	<ul style="list-style-type: none"><li>■ 新增了<a href="#">第 12 章 移轉至 vCloud Director 應用裝置</a>章節。</li><li>■ 新增了<a href="#">還原具有高可用性資料庫組態的 vCloud Director 應用裝置環境</a>主題。</li><li>■ 更新了<a href="#">應用裝置部署和資料庫高可用性組態</a>主題，以改善工作流程中的圖形和步驟 2。</li><li>■ 更新了<a href="#">檢查 vCloud Director 應用裝置中的記錄檔</a>主題，以新增包含部署 OVF 參數之檔案的相關資訊。</li></ul>
2019 年 3 月 28 日	初始版本。

# vCloud Director 安裝、組態及升級的概觀

# 1

您可以透過在一或多個 Linux 伺服器上安裝 vCloud Director 軟體或部署 vCloud Director 應用裝置的一或多個執行個體來建立 vCloud Director 伺服器群組。在安裝期間執行初始 vCloud Director 組態，包括建立網路與資料庫連線。

適用於 Linux 的 vCloud Director 軟體需要外部資料庫，而 vCloud Director 應用裝置使用內嵌式 PostgreSQL 資料庫。

建立 vCloud Director 伺服器群組後，將 vCloud Director 安裝與 vSphere 資源進行整合。對於網路資源，vCloud Director 可以使用 NSX Data Center for vSphere、NSX-T Data Center 或同時使用兩者。

升級現有 vCloud Director 安裝時，更新 vCloud Director 軟體和資料庫架構，保留伺服器、資料庫和 vSphere 之間的現有關係。

將 Linux 上的現有 vCloud Director 安裝移轉至 vCloud Director 應用裝置時，請更新 vCloud Director 軟體，並將資料庫移轉至應用裝置中的內嵌式資料庫。

本章節討論下列主題：

- [vCloud Director 架構](#)
- [組態規劃](#)

## vCloud Director 架構

vCloud Director 伺服器群組包含 Linux 上安裝的一或多個 vCloud Director 伺服器或 vCloud Director 應用裝置的部署。群組中的每個伺服器都會執行一組稱為 vCloud Director 儲存格的服務。所有儲存格共用單一 vCloud Director 資料庫和傳輸伺服器儲存區，並連線至 vSphere 和網路資源。

---

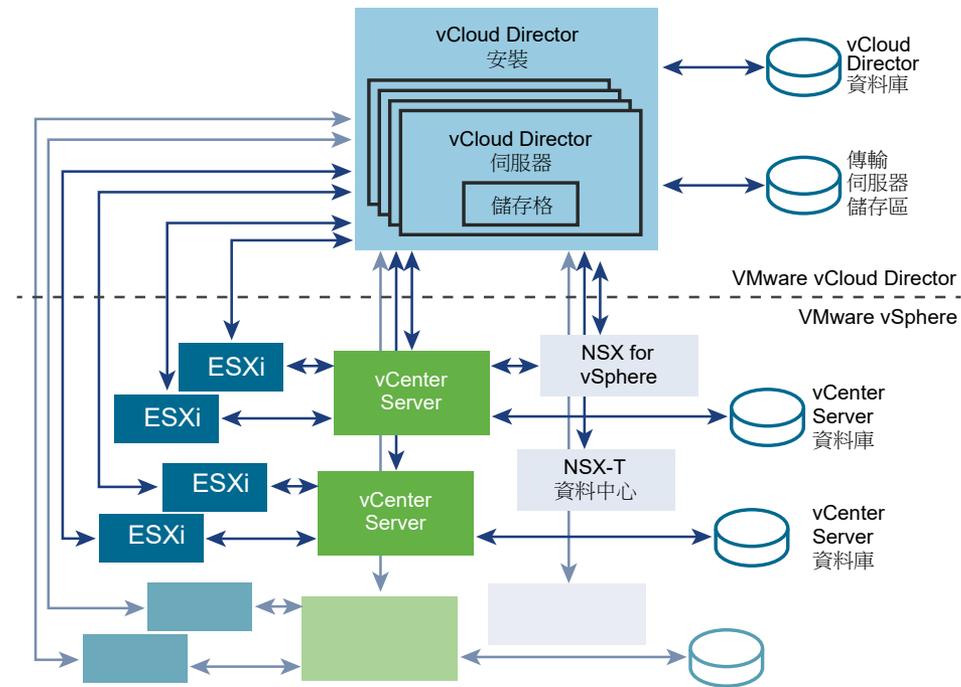
**重要** 不支援在同一個伺服器群組中的 Linux 和 vCloud Director 應用裝置部署上混合安裝 vCloud Director。

---

若要確保 vCloud Director 高可用性，您必須在伺服器群組中安裝至少兩個 vCloud Director 儲存格。當您使用第三方負載平衡器時，可確保在不停機的情況下自動進行容錯移轉。

您可以將 vCloud Director 安裝連線至多個 VMware vCenter Server<sup>®</sup> 系統及其管理的 VMware ESXi<sup>™</sup> 主機。對於網路服務，vCloud Director 可以使用與 vCenter Server 相關聯的 NSX Data Center for vSphere，也可以將 NSX-T Data Center 登錄到 vCloud Director。此外，也支援混合 NSX Data Center for vSphere 和 NSX-T Data Center。

圖 1-1. vCloud Director 架構圖表



Linux 上安裝的 vCloud Director 伺服器群組使用外部資料庫。

包含應用裝置部署的 vCloud Director 伺服器群組使用伺服器群組的第一個成員中的內嵌式資料庫。您可以透過將應用裝置的兩個執行個體部署為同一個伺服器群組中的待命儲存格，設定 vCloud Director 資料庫高可用性。請參閱 [應用裝置部署和資料庫高可用性組態](#)。

圖 1-2. 包含內嵌式資料庫高可用性叢集的 vCloud Director 應用裝置

vCloud Director 安裝和設定程序會建立儲存格、將儲存格連線至共用的資料庫和傳輸伺服器儲存區，並建立系統管理員帳戶。然後，系統管理員建立與 vCenter Server 系統、ESXi 主機和 NSX Manager 執行個體的連線。如需新增 vSphere 和網路資源的相關資訊，請參閱《vCloud Director 管理員指南》。

## 組態規劃

vSphere 提供 vCloud Director 的儲存、計算與網路容量。在開始安裝前，請先考量您的雲端需要的 vSphere 與 vCloud Director 容量，再規劃一個可支援的組態。

組態需求取決於許多因素，例如雲端上組織數目、每個組織的使用者數目以及前述使用者的活動等級。您可使用下列指南來開始進行大部分的組態：

- 針對每個要在雲端上使用的 vCenter Server 系統配置一個 vCloud Director 儲存格。
- 請確定所有目標 vCloud Director Linux 伺服器至少符合《vCloud Director 版本說明》中詳述的最低記憶體和儲存需求。
- 如果您計劃在 Linux 上安裝 vCloud Director，請設定 vCloud Director 資料庫，如 [準備 vCloud Director 資料庫](#) 中所述。

# vCloud Director 硬體及軟體需求

# 2

vCloud Director 伺服器群組中的每一個伺服器必須符合特定的硬體及軟體需求。此外，群組的所有成員必須能夠存取支援的資料庫。每個伺服器群組都需要存取 vCenter Server 系統、NSX Manager 執行個體以及一或多個 ESXi 主機。

## 其他 VMware 產品的相容性

如需有關 vCloud Director 和其他 VMware 產品之間相容性的最新資訊，請參閱《VMware 產品互通性對照表》，網址為 [http://partnerweb.vmware.com/comp\\_guide/sim/interop\\_matrix.php](http://partnerweb.vmware.com/comp_guide/sim/interop_matrix.php)。

## vSphere 組態需求

預期與 vCloud Director 搭配使用的 vCenter Server 執行個體和 ESXi 主機必須符合特定的組態需求。

- 預期用作 vCloud Director 外部網路或網路集區的 vCenter Server 網路，必須可由預期供 vCloud Director 使用的任何叢集中的所有主機使用。使這些網路可供資料中心的所有主機使用，可以簡化新增 vCenter Server 執行個體至 vCloud Director 的工作。
- NSX Data Center for vSphere 支援的隔離網路和網路集區需要 vSphere Distributed Switch。
- 搭配 vCloud Director 使用的 vCenter Server 叢集必須將 vSphere DRS 自動化層級指定為**全自動**。Storage DRS (若啟用) 可設定為任何自動化層級。
- vCenter Server 執行個體必須信任其主機。vCloud Director 管理的所有叢集中的所有主機必須設定為需要已驗證的主機憑證。尤其，您必須決定、比較及選取所有主機的相符指紋。請參閱《vCenter Server 和主機管理》說明文件中的「設定 SSL 設定」。

## vSphere 授權需求

vCloud Director Service Provider Bundle 包含必要的 vSphere 授權。

## 支援的平台、資料庫和瀏覽器

如需此版本的 vCloud Director 支援的伺服器平台、瀏覽器、LDAP 伺服器和資料庫的相關資訊，請參閱《vCloud Director 9.7 版本說明》。

## 磁碟空間、記憶體和 CPU 需求

vCloud Director 儲存格的磁碟空間、記憶體和 CPU 等實體需求均會列在《vCloud Director 9.7 版本說明》中。

## 共用儲存區

用於 vCloud Director 傳輸服務的 NFS 或其他共用儲存磁碟區。儲存磁碟區必須可擴充，並且可供伺服器群組中的所有伺服器存取。

本章節討論下列主題：

- [vCloud Director 的網路組態需求](#)
- [網路安全性需求](#)

## vCloud Director 的網路組態需求

vCloud Director 的正常運作必須仰賴安全、可靠的網路以支援正向及反向查閱主機名稱、網路時間服務以及其他服務。您的網路必須符合這些需求，然後您才能開始安裝 vCloud Director。

連線 vCloud Director 伺服器、資料庫伺服器、vCenter Server 系統及 NSX 元件的網路必須符合下列多個需求：

### IP 位址

每個 vCloud Director 伺服器都必須支援兩個不同的 SSL 端點。一個端點用於 HTTP 服務。另一個端點則用於主控台 Proxy 服務。這些端點可以是不同的 IP 位址，或是包含兩個不同連接埠的單一 IP 位址。您可以使用 IP 別名或多個網路介面來建立這些位址。請勿使用 Linux `ip addr add` 命令來建立第二個位址。

vCloud Director 應用裝置將具有自訂連接埠 8443 的 `eth0` IP 位址用於主控台 Proxy 服務。

### 主控台 Proxy 位址

設定為主控台 Proxy 端點的 IP 位址不得位於以 SSL 結尾的負載平衡器或反向 Proxy 後端。所有主控台 Proxy 要求必須直接轉送至主控台 Proxy IP 位址。

對於使用單一 IP 位址的安裝，可以從 vCloud Director Web 主控台自訂主控台 Proxy 位址。例如，對於 vCloud Director 應用裝置，您必須將主控台 Proxy 位址自訂為 `vcloud.example.com:8443`。

### 網路時間服務

您必須使用網路時間服務 (例如 NTP)，才能同步所有 vCloud Director 伺服器的時鐘，包括資料庫伺服器。已同步伺服器的時鐘之間的可允許偏移上限為 2 秒。

### 伺服器時區

包括資料庫伺服器在內的所有 vCloud Director 伺服器都必須設定為在相同的時區內。

### 主機名稱解析

DNS 必須可以正向及反向查閱完整網域名稱或未限定主機名稱，解析所有您在安裝及設定期間指定的主機名稱。例如，對於名為 `vcloud.example.com` 的主機，下列兩個命令必須接在 vCloud Director 主機後面：

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

此外，如果主機 `vcloud.example.com` 的 IP 位址為 `192.168.1.1`，則下列命令必須傳回 `vcloud.example.com`：

```
nslookup 192.168.1.1
```

應用裝置需要對 `eth0` IP 位址進行反向 DNS 查閱。必須在您的環境中成功執行下列命令：

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

## 網路安全性需求

vCloud Director 的安全作業需要安全的網路環境。設定並測試此網路環境，然後再開始安裝 vCloud Director

將所有 vCloud Director 伺服器連線至安全且受到監控的網路。vCloud Director 網路連線具有數個額外的需求：

- 不要將 vCloud Director 直接連線至公用網際網路。一律使用防火牆來保護 vCloud Director 網路連線。連接埠 443 (HTTPS) 必須只對傳入連線開啟。必要時，連接埠 22 (SSH) 及 80 (HTTP) 也可以對傳入連線開啟。此外，`cell-management-tool` 還需要存取儲存格的回送位址。防火牆必須拒絕來自公用網路的所有其他傳入流量，包括 JMX 要求 (連接埠 8999) 在內。

表 2-1. 必須允許來自 vCloud Director 主機的傳入封包的連接埠

連接埠	通訊協定	註解
111	TCP、UDP	傳輸服務所使用的 NFS 連接埠對應程式
920	TCP、UDP	傳輸服務所使用的 NFS <code>rpc.statd</code>
61611	TCP	AMQP
61616	TCP	AMQP

- 不要將用於傳出連線的連接埠連線至公用網路。

表 2-2. 必須允許來自 vCloud Director 主機的傳出封包的連接埠

連接埠	通訊協定	註解
25	TCP、UDP	SMTP
53	TCP、UDP	DNS
111	TCP、UDP	傳輸服務所使用的 NFS 連接埠對應程式
123	TCP、UDP	NTP
389	TCP、UDP	LDAP

表 2-2. 必須允許來自 vCloud Director 主機的傳出封包的連接埠 (續)

連接埠	通訊協定	註解
443	TCP	使用標準連接埠的 vCenter、NSX Manager 以及 ESXi 連線。如果您已為這些服務選擇不同的連接埠，請停用連接埠 443 的連線，然後針對選擇的連接埠進行啟用。
514	UDP	選擇性。啟用 Syslog 使用。
902	TCP	vCenter 及 ESXi 連線。
903	TCP	vCenter 及 ESXi 連線。
920	TCP、UDP	傳輸服務所使用的 NFS rpc.statd。
1433	TCP	預設 Microsoft SQL Server 資料庫連接埠。
5672	TCP、UDP	選擇性。用於工作延伸的 AMQP 訊息。
61611	TCP	AMQP
61616	TCP	AMQP

- 透過專用私人網路路由 vCloud Director 伺服器與以下伺服器之間的流量。
  - vCloud Director 資料庫伺服器
  - RabbitMQ
  - Cassandra
- 如果可能，透過專用私人網路路由 vCloud Director 伺服器、vSphere 與 NSX 之間的流量。
- 虛擬交換器與支援提供者網路的分散式虛擬交換器必須彼此隔離。它們無法共用相同的第 2 層實體網路區段。
- 將 NFSv4 用於傳輸服務儲存區。最常見的 NFS 版本 NFSv3 不會提供「傳輸中加密」，在某些組態中，此加密可能會針對正在傳輸的資料啟用傳遞探查或竄改。SANS 白皮書《[受信任和不信任環境中的 NFS 安全性](#)》說明了 NFSv3 的固有威脅。可從 VMware 知識庫文章 [2086127](#) 中取得有關設定和保護 vCloud Director 傳輸服務之安全的其他資訊。

# 安裝 vCloud Director 或部署 vCloud Director 應用裝置之前

# 3

在 Linux 伺服器上安裝 vCloud Director 或部署 vCloud Director 應用裝置之前，必須先準備環境。

本章節討論下列主題：

- [準備 vCloud Director 資料庫](#)
- [準備傳輸伺服器儲存區](#)
- [下載並安裝 VMware 公用金鑰](#)
- [為 vCloud Director 安裝和設定 NSX Data Center for vSphere](#)
- [為 vCloud Director 安裝和設定 NSX-T Data Center](#)

## 準備 vCloud Director 資料庫

vCloud Director 儲存格會使用資料庫來儲存共用資訊。在 Linux 上安裝 vCloud Director 之前，您必須安裝並設定外部 vCloud Director 資料庫。vCloud Director 應用裝置使用內嵌式 PostgreSQL 資料庫。

如需有關支援的 vCloud Director 資料庫的資訊，請參閱《[VMware 產品互通性對照表](#)》。

無論您決定使用哪一個資料庫軟體，都必須建立個別專用的資料庫架構，以供 vCloud Director 使用。vCloud Director 無法與其他任何 VMware 產品共用資料庫架構。

---

**重要** vCloud Director 僅支援 SSL 連線至 PostgreSQL 資料庫。在自動網路及資料庫連線設定期間或建立 vCloud Director 伺服器群組後，您可以在 PostgreSQL 資料庫上啟用 SSL。請參閱 [自動組態參考與在外部 PostgreSQL 資料庫上執行其他組態](#)。

---

## 在 Linux 上設定 vCloud Director 的外部 PostgreSQL 資料庫

將 PostgreSQL 資料庫與 vCloud Director 搭配使用時，PostgreSQL 資料庫需符合特定組態需求。在 Linux 上安裝 vCloud Director 前，必須安裝和設定資料庫執行個體，並建立 vCloud Director 資料庫使用者帳戶。

---

**備註** 僅 Linux 上的 vCloud Director 使用外部資料庫。vCloud Director 應用裝置使用內嵌式 PostgreSQL 資料庫。

---

### 必要條件

您必須熟悉 PostgreSQL 命令、指令碼與作業。

**程序****1** 設定資料庫伺服器。

具有 16 GB 記憶體、100 GB 儲存區和 4 個 CPU 的資料庫伺服器適用於一般 vCloud Director 伺服器群組。

**2** 在資料庫伺服器上安裝支援的 PostgreSQL 發行版。

- 資料庫的 `SERVER_ENCODING` 值必須為 `UTF-8`。如果安裝資料庫，並始終符合資料庫伺服器作業系統所使用的編碼，則會建立此值。
- 使用 PostgreSQL `initdb` 命令，將 `LC_COLLATE` 和 `LC_CTYPE` 的值設定為 `en_US.UTF-8`。例如：

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

**3** 建立資料庫使用者。

下列命令會建立使用者 `vcloud`。

```
create user vcloud;
```

**4** 建立資料庫執行個體並為其指定擁有者。

使用類似下列內容的命令，將名為 `vcloud` 的資料庫使用者指定為資料庫擁有者。

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

**5** 將資料庫密碼指派給資料庫擁有者帳戶。

以下命令會將密碼 `vcloudpass` 指派給資料庫擁有者 `vcloud`。

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

**6** 可讓資料庫擁有者登入資料庫。

以下命令會將 `login` 選項指派給資料庫擁有者 `vcloud`。

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

**後續步驟**

建立 vCloud Director 伺服器群組後，您可以將 PostgreSQL 資料庫設定為需要來自 vCloud Director 儲存格的 SSL 連線，並調整部分資料庫參數以獲得最佳效能。請參閱[在外部 PostgreSQL 資料庫上執行其他組態](#)。

**設定 Linux 版 vCloud Director 的外部 Microsoft SQL Server 資料庫**

在搭配 SQL Server 資料庫與 vCloud Director 使用時需符合特定組態需求。在 Linux 上安裝 vCloud Director 前，必須安裝和設定資料庫執行個體，並建立 vCloud Director 資料庫使用者帳戶。

vCloud Director 資料庫效能是整體 vCloud Director 效能與延展性的重要因素之一。vCloud Director 使用 SQL Server `tmpdb` 檔案來儲存大型結果集、排序資料與管理資料的同步讀取與修改動作。當 vCloud Director 的同時負載量過大時，該檔案也將變得過於龐大。所以建議您將 `tmpdb` 檔案建立在讀寫效能快的專用磁碟區。如需關於 `tmpdb` 檔案與 SQL Server 效能的詳細資訊，請參閱 <http://msdn.microsoft.com/en-us/library/ms175527.aspx>。

**備註** 僅 Linux 上的 vCloud Director 使用外部資料庫。vCloud Director 應用裝置使用內嵌式 PostgreSQL 資料庫。

#### 必要條件

- 您必須熟悉 Microsoft SQL Server 命令、指令檔與作業。
- 若要設定 Microsoft SQL Server，請先使用管理員認證登入 SQL Server 主機電腦。SQL Server 可設定為以 `LOCAL_SYSTEM` 身分識別或是任何可執行 Windows 服務權限的身分識別來執行。
- 如需 Microsoft SQL Server Always On Availability Groups 與 vCloud Director 資料庫搭配使用的相關資訊，請參閱 VMware 知識庫文章 <https://kb.vmware.com/kb/2148767>。

#### 程序

##### 1 設定資料庫伺服器。

記憶體 16 GB、儲存區 100 GB 且配有 4 個 CPU 的資料庫伺服器對多數 vCloud Director 伺服器群組來說應該足夠了。

##### 2 在 SQL Server 安裝期間請指定使用混合模式驗證。

在搭配 SQL Server 與 vCloud Director 使用時無法支援 Windows 驗證。

##### 3 建立資料庫執行個體。

下列指令檔用來建立資料庫與記錄檔，並指定適用的定序序列。

```
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
```

上方顯示的 `SIZE` 值僅為建議值。您可能必須使用較大的值。

##### 4 設定交易隔離等級。

下列指令檔將交易隔離等級設定為 `READ_COMMITTED_SNAPSHOT`。

```
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
```

如需關於交易隔離的詳細資訊，請參閱 <http://msdn.microsoft.com/en-us/library/ms173763.aspx>。

## 5 建立 vCloud Director 資料庫使用者帳戶。

下列指令檔用來建立資料庫使用者名稱 `vcloud`，密碼 `vcloudpass`。

```
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 為 vCloud Director 資料庫使用者帳戶指定權限。

下列指令檔將 `db_owner` 角色指定給 [步驟 5](#) 中建立的資料庫使用者。

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

# 準備傳輸伺服器儲存區

若要提供暫存儲存區進行上傳、下載以及儲存外部發佈或訂閱的目錄項目，您必須使 vCloud Director 伺服器群組中的所有伺服器都能存取 NFS 或其他共用儲存磁碟區。

**重要** vCloud Director 應用裝置僅支援 NFS 類型的共用儲存區。應用裝置部署程序涉及掛接 NFS 共用傳輸伺服器儲存區。

將 NFS 用於傳輸伺服器儲存區時，您必須設定 vCloud Director 伺服器群組中的每個 vCloud Director 儲存格，以掛接和使用以 NFS 為基礎的傳輸伺服器儲存區。您需要特定的使用者和群組權限來設定每個儲存格，以掛接以 NFS 為基礎的位置，並將其用作傳輸伺服器儲存區。

伺服器群組的每一個成員都會將此磁碟區掛接到同一個掛接點，通常是 `/opt/vmware/vcloud-director/data/transfer`。消耗此磁碟區空間的方式有兩種：

- 傳輸期間，上傳和下載內容均佔用此儲存區。傳輸完成後，將從儲存區中移除上傳和下載內容。閒置達 60 分鐘的傳輸會標記為到期並且會由系統清除。傳輸的影像可能很大，所以最好至少配置數百 GB 供使用。

- 在外部發佈且啟用已發佈內容快取的目錄中的目錄項目會佔用此儲存區。在外部發佈但未啟用快取的目錄中的項目不會佔用此儲存區。如果允許雲端中的組織建立在外部發佈的目錄，您可以假設數百或甚至數千個目錄項目需要此磁碟區上的空間。每個目錄項目的大小約為壓縮 OVF 形式的虛擬機器大小。

**備註** 傳輸伺服器儲存區的磁碟區必須具有用於進一步擴充的容量。

## vCloud Director 在傳輸伺服器儲存區位置上如何使用檔案系統權限

對於 vCloud Director 伺服器群組中的所有 vCloud Director 儲存格：

- 在標準雲端作業 (例如將項目上傳至目錄) 中，vCloud Director 儲存格的精靈會使用 **vcloud** 群組中的 **vcloud** 使用者，將檔案寫入傳輸伺服器儲存區並從此儲存區中讀取這些檔案。**vcloud** 使用者透過 `umask 0077` 寫入檔案。當 vCloud Director 安裝程式在伺服器群組成員上執行並安裝 vCloud Director 軟體時，它也會建立 **vcloud** 使用者和 **vcloud** 群組。
- vCloud Director 記錄資料收集器指令碼 `vmware-vcd-support` 可在一項作業中從所有 vCloud Director 儲存格收集記錄，並將記錄組合至單一 `tar.gz` 檔案中。當您執行指令碼時，它會使用叫用指令碼之使用者的使用者識別碼，將產生的 `tar.gz` 檔案寫入至傳輸伺服器儲存區位置中的目錄。依預設，具有執行指令碼權限的唯一使用者是 **root** 使用者。
- 儲存格上的 **root** 使用者執行指令碼，將 `tar.gz` 檔案寫入至傳輸伺服器儲存區位置中的 `vmware-vcd-support` 目錄。如果您想要使用多儲存格選項同時從所有儲存格收集記錄，則 **root** 使用者必須具有讀取權限，才能擷取 `tar.gz` 診斷記錄服務包。

## 設定 NFS 伺服器的需求

設定 NFS 伺服器有特定的需求，以便 vCloud Director 能夠將檔案寫入以 NFS 為基礎的傳輸伺服器儲存區位置，並從該位置讀取檔案。因此，**vcloud** 使用者可以執行標準雲端作業，而 **root** 使用者可以執行多儲存格記錄收集。

- NFS 伺服器的匯出清單必須允許 vCloud Director 伺服器群組中的每個伺服器成員對匯出清單中所識別的共用位置具有讀取寫入權限。此功能可讓 **vcloud** 使用者將檔案寫入共用位置，並從該位置讀取檔案。
- NFS 伺服器必須允許 vCloud Director 伺服器群組中的每個伺服器上的 **root** 系統帳戶對共用位置具有讀取寫入權限。此功能可讓您使用 `vmware-vcd-support` 指令碼及其多儲存格選項，在單一服務包中同時從所有儲存格收集記錄。您可以針對此共用位置在 NFS 匯出組態中使用 `no_root_squash` 來滿足此需求。

例如，如果 NFS 伺服器具有 IP 位址 192.168.120.7，並將名為 `vCDspace` 的目錄做為 vCloud Director 伺服器群組 (位置為 `/nfs/vCDspace`) 的傳輸空間，若要匯出此目錄，則必須確保其擁有權和權限為 **root:root** 和 **750**。允許對名為 `vcd-cell1-IP` 和 `vcd-cell2-IP` 的兩個儲存格的共用位置進行讀取寫入的方法是 `no_root_squash` 方法。您必須在 `/etc/exports` 檔案中新增一行。

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

在匯出行程中，各個儲存格 IP 位址與其緊接的左括弧之間不得有空格。如果 NFS 伺服器在儲存格將資料寫入共用位置時重新開機，則在匯出組態中使用 `sync` 選項可防止共用位置中出現資料損毀情況。匯出檔案系統的子目錄時，在匯出組態中使用 `no_subtree_check` 選項可提高可靠性。

必須允許 vCloud Director 伺服器群組中的每個伺服器透過檢查 NFS 匯出的匯出清單來掛接 NFS 共用。您可以透過執行 `exportfs -a` 重新匯出所有 NFS 共用以匯出掛接。NFS 精靈 `rpcinfo -p localhost` 或 `service nfs status` 必須在伺服器上執行。

## 規劃將 vCloud Director 安裝升級至更新版本時的考量事項

在升級 vCloud Director 伺服器群組期間，您可以針對已升級的版本執行安裝檔案，以升級 vCloud Director 伺服器群組的所有成員。為了方便起見，某些組織會選擇下載安裝檔案以升級到傳輸伺服器儲存區位置，並從該處執行安裝檔案，因為所有儲存格都有權存取該位置。由於必須使用 **root** 使用者執行升級安裝檔案，如果您想要使用傳輸伺服器儲存區位置執行升級，則必須確保 **root** 使用者可以在您執行升級時執行升級安裝檔案。如果您無法以 **root** 使用者身分執行升級，則必須將該檔案複製到可以 **root** 使用者身分執行的其他位置，例如，位於 NFS 掛接外部的其他目錄。

## 下載並安裝 VMware 公用金鑰

安裝檔案是以數位方式簽署的。若要驗證簽章，您必須下載並安裝 VMware 公用金鑰。

您可以使用 Linux `rpm` 工具及 VMware 公用金鑰，驗證 vCloud Director 安裝檔案的數位簽章，或任何來自 `vmware.com` 的其他已簽署下載檔案。如果您在打算安裝 vCloud Director 的電腦上安裝公用金鑰，則會在安裝或升級時進行驗證。您也可以開始安裝或升級程序之前手動驗證簽章，然後使用已驗證的檔案進行所有安裝或升級。

---

**備註** 下載網站也會發佈下載的總和檢查值。總和檢查是以兩種常用的形式來發佈。驗證總和檢查會驗證您下載的內容是否與公佈的內容相同。它不會驗證數位簽章。

---

### 程序

- 1 建立目錄來儲存 VMware 封裝公用金鑰。
- 2 使用網頁瀏覽器，從 <http://packages.vmware.com/tools/keys> 目錄下載所有的 VMware 公用封裝公用金鑰。
- 3 將金鑰檔儲存至您建立的目錄。
- 4 對於每一個您下載的金鑰，請執行下列命令來匯入金鑰。

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

`key_path` 是儲存金鑰的目錄。

`key_name` 是金鑰的檔名。

## 為 vCloud Director 安裝和設定 NSX Data Center for vSphere

如果您想要 vCloud Director 安裝使用 NSX Data Center for vSphere 的網路資源，則必須安裝和設定 NSX Data Center for vSphere 並將唯一的 NSX Manager 執行個體與您打算包含在 vCloud Director 安裝中的每個 vCenter Server 執行個體相關聯。

NSX Manager 包含在 NSX Data Center for vSphere 下載中。如需有關 vCloud Director 和其他 VMware 產品之間相容性的最新資訊，請參閱《VMware 產品互通性對照表》，網址為 [http://partnerweb.vmware.com/comp\\_guide/sim/interop\\_matrix.php](http://partnerweb.vmware.com/comp_guide/sim/interop_matrix.php)。如需網路需求的相關資訊，請參閱 vCloud Director 的網路組態需求。

---

**重要** 此程序僅在執行 vCloud Director 的全新安裝時才適用。如果您是要升級現有的 vCloud Director 安裝，請參閱第 11 章 [升級 vCloud Director](#) 和 [修補 vCloud Director 應用裝置](#)。

---

### 必要條件

確認每個 vCenter Server 系統均符合安裝 NSX Manager 的必要條件。

### 程序

- 1 執行 NSX Manager 虛擬應用裝置的安裝工作。  
請參閱《NSX 安裝指南》。
- 2 登入您所安裝的 NSX Manager 虛擬應用裝置，並確認您在安裝期間指定的設定。
- 3 讓您所安裝的 NSX Manager 虛擬應用裝置與您打算在規劃的 vCloud Director 安裝中新增至 vCloud Director 的 vCenter Server 系統產生關聯。
- 4 在相關聯的 NSX Manager 執行個體中設定 VXLAN 支援。  
vCloud Director 會建立 VXLAN 網路集區，以提供網路資源給提供者 VDC。如果未在相關聯的 NSX Manager 中設定 VXLAN 支援，則提供者 VDC 會顯示網路集區錯誤，此時您必須建立不同類型的網路集區，並將其與提供者 VDC 相關聯。如需有關設定 VXLAN 支援的詳細資訊，請參閱《NSX 管理指南》。
- 5 (選擇性) 如果您想要系統中的 Edge 閘道提供分散式路由，請設定 NSX Controller 叢集。  
請參閱《NSX 管理指南》。

## 為 vCloud Director 安裝和設定 NSX-T Data Center

如果您想要 vCloud Director 安裝使用來自 NSX-T Data Center 的網路資源，則必須安裝 NSX-T Data Center 並設定至少一個 NSX-T Manager 執行個體。

NSX-T Manager 包含在 NSX-T Data Center 下載中。如需有關 vCloud Director 和其他 VMware 產品之間相容性的最新資訊，請參閱《VMware 產品互通性對照表》，網址為 [http://partnerweb.vmware.com/comp\\_guide/sim/interop\\_matrix.php](http://partnerweb.vmware.com/comp_guide/sim/interop_matrix.php)。如需網路需求的相關資訊，請參閱 vCloud Director 的網路組態需求。

---

**重要** 此程序僅在執行 vCloud Director 的全新安裝時才適用。如果您是要升級現有的 vCloud Director 安裝，請參閱第 11 章 [升級 vCloud Director](#) 和 [修補 vCloud Director 應用裝置](#)。

---

### 必要條件

您必須熟悉 NSX-T Data Center。

### 程序

- 1 安裝 NSX-T Manager 虛擬應用裝置。  
請參閱《NSX-T 安裝指南》。
- 2 準備要與 NSX-T Data Center 共同運作的 ESXi 主機。  
請參閱《NSX-T 安裝指南》。
- 3 根據雲端需求建立傳輸節點和傳輸區域。  
請參閱《NSX-T 安裝指南》。
- 4 設定邊緣節點和叢集。  
請參閱《NSX-T 安裝指南》。
- 5 設定第 0 層和第 1 層路由器。  
請參閱《NSX-T 管理指南》。
- 6 設定要匯入至 vCloud Director 安裝中的一或多個 VLAN 或覆疊邏輯交換器。  
請參閱《NSX-T 管理指南》。

### 後續步驟

安裝 vCloud Director 後，您可以將 NSX-T Manager 執行個體登錄到雲端。如需登錄 NSX-T Manager 執行個體的相關資訊，請參閱《服務提供者適用的 vCloud API 程式設計指南》。

# 針對 Linux 上的 vCloud Director 建立和管理 SSL 憑證

# 4

vCloud Director 使用 SSL 保護用戶端與伺服器之間通訊的安全。每個 vCloud Director 伺服器必須支援兩個不同的 SSL 端點，分別用於 HTTPS 和主控台 Proxy 通訊。

這些端點可以是不同的 IP 位址，也可以是包含兩個不同連接埠的單一 IP 位址。每個端點均需要其專屬的 SSL 憑證。您可以針對兩個端點使用相同的憑證，例如，使用萬用字元憑證。

本章節討論下列主題：

- 為 Linux 上的 vCloud Director 建立 SSL 憑證之前
- 為 Linux 上的 vCloud Director 建立自我簽署的 SSL 憑證
- 為 Linux 上的 vCloud Director 建立 CA 簽署的 SSL 憑證金鑰儲存區
- 為 Linux 上的 vCloud Director 建立包含已匯入私密金鑰的 CA 簽署的 SSL 憑證金鑰儲存區

## 為 Linux 上的 vCloud Director 建立 SSL 憑證之前

安裝適用於 Linux 的 vCloud Director 時，您必須為伺服器群組的每個成員建立兩個憑證，然後將這些憑證匯入主機金鑰儲存區中。

**備註** 您必須在 Linux 上安裝 vCloud Director 後，才能為伺服器群組成員建立憑證。vCloud Director 應用裝置會在首次開機期間建立自我簽署的 SSL 憑證。

### 程序

- 1 以 **root** 身分登入 vCloud Director 伺服器。
- 2 列出伺服器的 IP 位址。  
使用諸如 `ifconfig` 等命令來搜尋此伺服器的 IP 位址。
- 3 對於每個 IP 位址，請執行下列命令以擷取 IP 位址繫結的完整網域名稱 (FQDN)。

```
nslookup ip-address
```

- 4 記下每個 IP 位址及其相關聯的 FQDN。如果未針對兩個服務使用單一 IP 位址，請決定將哪個 IP 位址用於 HTTPS 服務，將哪個 IP 位址用於主控台 Proxy 服務。

建立憑證時必須提供 FQDN，而設定網路及資料庫連線時必須提供 IP 位址。記下可存取 IP 位址的任何其他 FQDN，因為如果想要憑證包含主體別名，就必須提供 FQDN。

## 後續步驟

為兩個端點建立憑證。您可以使用由信任憑證授權機構 (CA) 簽署的憑證或是自我簽署憑證。

**備註** CA 簽署的憑證是信任等級最高的憑證。

- 如需建立和匯入 CA 簽署的 SSL 憑證的相關資訊，請參閱[為 Linux 上的 vCloud Director 建立 CA 簽署的 SSL 憑證金鑰儲存區](#)。
- 如需建立自我簽署 SSL 憑證的相關資訊，請參閱[為 Linux 上的 vCloud Director 建立自我簽署的 SSL 憑證](#)。
- 如需匯入您自己的私密金鑰和 CA 簽署的憑證檔案的相關資訊，請參閱[為 Linux 上的 vCloud Director 建立包含已匯入私密金鑰的 CA 簽署的 SSL 憑證金鑰儲存區](#)。

## 為 Linux 上的 vCloud Director 建立自我簽署的 SSL 憑證

在高度信任的環境下，自我簽署憑證可提供一個較為便利的方式來為 vCloud Director 設定 SSL。

每個 vCloud Director 伺服器都要求 JCEKS 金鑰儲存區檔案中有兩個 SSL 憑證，一個用於 HTTPS 服務，另一個則用於主控台 Proxy 服務。

您可以使用 `cell-management-tool` 建立自我簽署的 SSL 憑證。在執行組態代理程式之前及執行安裝檔案之後，`cell-management-tool` 公用程式會安裝在儲存格上。請參閱[在伺服器群組的第一個成員上安裝 vCloud Director 軟體](#)。

**重要** 這些範例指定 2048 位元的金鑰大小，但是您應當先評估安裝的安全需求，然後再選擇適當的金鑰大小。根據 NIST 特刊 800-131A，小於 1024 位元的金鑰大小不再受到支援。

### 程序

- 1 以 **root** 身分直接登入或使用 SSH 用戶端登入 vCloud Director 伺服器的作業系統。
- 2 執行命令，為 HTTPS 服務和主控台 Proxy 服務建立公用和私密金鑰配對。

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

此命令會在 `certificates.ks` 建立或更新密碼為 `passwd` 的金鑰儲存區。`cell-management-tool` 使用命令的預設值建立憑證。視環境的 DNS 組態而定，簽發者 CN 將設定為每個服務的 IP 位址或 FQDN。此憑證使用預設的 2048 位元金鑰長度，並在建立後一年到期。

**重要** 金鑰儲存區檔案及其儲存目錄必須可供使用者 **vcloud.vcloud** 讀取。vCloud Director 安裝程式會建立此使用者和群組。

## 後續步驟

記下金鑰儲存區路徑名稱。當您執行組態指令碼來建立 vCloud Director 儲存格的網路和資料庫連線時，需要提供金鑰儲存區路徑名稱。請參閱[設定網路與資料庫連線](#)。

## 為 Linux 上的 vCloud Director 建立 CA 簽署的 SSL 憑證金鑰儲存區

建立與匯入 CA 簽署的憑證為 SSL 通訊提供了最高層級的信任，並有助於保護雲端基礎結構內的連線安全。

每個 vCloud Director 伺服器都需要兩個 SSL 憑證，才能確保用戶端與伺服器之間安全通訊。每個 vCloud Director 伺服器必須支援兩個不同的 SSL 端點，分別用於 HTTPS 和主控台 Proxy 通訊。

這兩個端點可以是不同的 IP 位址，也可以是包含兩個不同連接埠的單一 IP 位址。每個端點均需要其專屬的 SSL 憑證。您可以針對兩個端點使用相同的憑證，例如，使用萬用字元憑證。

兩個端點的憑證皆必須包含 X.500 辨別名稱和 X.509 主體別名延伸。

您可以使用由信任憑證授權機構 (CA) 簽署的憑證或是自我簽署憑證。

您可以使用 `cell-management-tool` 建立自我簽署的 SSL 憑證。在執行組態代理程式之前及執行安裝檔案之後，`cell-management-tool` 公用程式會安裝在儲存格上。請參閱[在伺服器群組的第一個成員上安裝 vCloud Director 軟體](#)。

如果您已有個人私密金鑰和 CA 簽署的憑證檔案，請依照[為 Linux 上的 vCloud Director 建立包含已匯入私密金鑰的 CA 簽署的 SSL 憑證金鑰儲存區](#)中所述的程序進行操作。

---

**重要** 這些範例指定 2048 位元的金鑰大小，但是您應當先評估安裝的安全需求，然後再選擇適當的金鑰大小。根據 NIST 特刊 800-131A，小於 1024 位元的金鑰大小不再受到支援。

---

### 必要條件

- 請確認您有權存取已安裝 Java Runtime Environment 8 或更新版本的電腦，以便使用 `keytool` 命令來匯入憑證。vCloud Director 安裝程式會將 `keytool` 的複本置於 `/opt/vmware/vcloud-director/jre/bin/keytool`，但是您可以在任何已安裝 Java Runtime Environment 的電腦上執行此程序。不支援利用任何其他來源之 `keytool` 所建立的憑證與 vCloud Director 搭配使用。這些命令列範例假設 `keytool` 已位於使用者路徑中。
- 自行熟悉 `keytool` 命令。
- 如需有關 `generate-certs` 命令之可用選項的更多詳細資料，請參閱 [〈為 HTTPS 和主控台 Proxy 端點產生自我簽署憑證〉](#)。
- 如需有關 `certificates` 命令之可用選項的更多詳細資料，請參閱 [〈取代 HTTP 和主控台 Proxy 端點的憑證〉](#)。

### 程序

- 1 以 **root** 身分直接登入或使用 SSH 用戶端登入 vCloud Director 伺服器儲存格的作業系統。
- 2 執行命令，為 HTTPS 服務和主控台 Proxy 服務建立公用和私密金鑰配對。

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

此命令會在 `certificates.ks` 建立或更新具有指定密碼的金鑰儲存區。已使用命令的預設值建立憑證。視環境的 DNS 組態而定，簽發者 CN 將設定為每個服務的 IP 位址或 FQDN。此憑證使用預設的 2048 位元金鑰長度，並在建立後一年到期。

**重要** 金鑰儲存區檔案及其儲存目錄必須可供使用者 `vcloud.vcloud` 讀取。vCloud Director 安裝程式會建立此使用者和群組。

### 3 為 HTTPS 服務和主控台 Proxy 服務建立憑證簽署要求。

**重要** 如果您針對 HTTPS 服務和主控台 Proxy 服務使用不同的 IP 位址，請在下列命令中調整主機名稱和 IP 位址。

#### a 在 `http.csr` 檔案中建立憑證簽署要求。

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

#### b 在 `consoleproxy.csr` 檔案中建立憑證簽署要求。

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

### 4 傳送憑證簽署要求到您的憑證授權機構。

如果您的憑證授權單位要求您指定網頁伺服器類型，請使用 Jakarta Tomcat。

取得 CA 簽署憑證。

### 5 將簽署憑證匯入 JCEKS 金鑰儲存區。

#### a 將憑證授權機構的根憑證從 `root.cer` 檔案匯入到 `certificates.ks` 金鑰儲存區檔案中。

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

#### b 如果收到了中繼憑證，請將其從 `intermediate.cer` 檔案匯入到 `certificates.ks` 金鑰儲存區檔案中。

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

- c 匯入 HTTPS 服務憑證。

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

- d 匯入主控台 Proxy 服務憑證。

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

此命令使用新取得的 CA 簽署的憑證版本來覆寫 `certificates.ks` 檔案。

- 6 若要確認憑證是否已匯入至 JCEKS 金鑰儲存區，請執行命令以列出金鑰儲存區檔案的內容。

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

- 7 對伺服器群組中的所有 vCloud Director 伺服器重複此程序。

#### 後續步驟

- 如果您尚未設定 vCloud Director 執行個體，請執行 `configure` 指令碼，將憑證金鑰儲存區匯入至 vCloud Director。請參閱[設定網路與資料庫連線](#)。

**備註** 如果您建立的 `certificates.ks` keystore 檔案所在電腦與您產生完整網域名稱與相關 IP 位址清單的所在伺服器不同，請立即將該 keystore 檔案複製到該伺服器。執行組態指令檔時，您需要提供該金鑰儲存區路徑名稱。

- 如果您已安裝並設定 vCloud Director 執行個體，請使用儲存格管理工具的 `certificates` 命令匯入憑證金鑰儲存區。請參閱〈[取代 HTTP 和主控台 Proxy 端點的憑證](#)〉。

## 為 Linux 上的 vCloud Director 建立包含已匯入私密金鑰的 CA 簽署的 SSL 憑證金鑰儲存區

如果您有自己的私密金鑰和 CA 簽署的憑證檔案，必須在 vCloud Director 環境中匯入金鑰儲存區之前，建立用於匯入 HTTPS 和主控台 Proxy 服務的憑證和私密金鑰的金鑰儲存區檔案。

#### 必要條件

- 請參閱[為 Linux 上的 vCloud Director 建立 SSL 憑證之前](#)。
- 請確認您有權存取已安裝 Java Runtime Environment 8 或更新版本的電腦，以便使用 `keytool` 命令來匯入憑證。vCloud Director 安裝程式會將 `keytool` 的複本置於 `/opt/vmware/vcloud-director/jre/bin/keytool`，但是您可以在任何已安裝 Java Runtime Environment 的電腦上執行此程序。不支援利用任何其他來源之 `keytool` 所建立的憑證與 vCloud Director 搭配使用。這些命令列範例假設 `keytool` 已位於使用者路徑中。
- 自行熟悉 `keytool` 命令。
- 下載並安裝 OpenSSL。

- 如需有關 `certificates` 命令之可用選項的更多詳細資料，請參閱〈[取代 HTTP 和主控台 Proxy 端點的憑證](#)〉。

## 程序

- 1 如果您有中繼憑證，請執行命令，將根 CA 簽署的憑證與中繼憑證組合在一起，並建立憑證鏈結。

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

- 2 使用 OpenSSL 為 HTTPS 和主控台 Proxy 服務建立具有私密金鑰、憑證鏈結和相應別名的中繼 PKCS12 金鑰儲存區檔案，並為每個金鑰儲存區檔案指定密碼。

- a 為 HTTPS 服務建立金鑰儲存區檔案。

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

- b 為主控台 Proxy 服務建立金鑰儲存區檔案。

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

- 3 使用 `keytool` 將 PKCS12 金鑰儲存區匯入至 JCEKS 金鑰儲存區。

- a 執行命令以匯入 HTTPS 服務的 PKCS12 金鑰儲存區。

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

- b 執行命令以匯入主控台 Proxy 服務的 PKCS12 金鑰儲存區。

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

- 4 若要確認憑證是否已匯入至 JCEKS 金鑰儲存區，請執行命令以列出金鑰儲存區檔案的內容。

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

- 5 對環境中的所有 vCloud Director 儲存格重複此程序。

## 後續步驟

- 如果您尚未設定 vCloud Director 執行個體，請執行 `configure` 指令碼，將憑證金鑰儲存區匯入至 vCloud Director。請參閱[設定網路與資料庫連線](#)。

---

**備註** 如果您建立的 `certificates.ks` 金鑰儲存區檔案所在電腦與您產生完整網域名稱與相關 IP 位址清單的所在伺服器不同，請將該金鑰儲存區檔案複製到該伺服器。執行組態指令檔時，您需要提供該金鑰儲存區路徑名稱。

---

- 如果您已安裝並設定 vCloud Director 執行個體，請使用儲存格管理工具的 `certificates` 命令匯入憑證金鑰儲存區。請參閱 [〈取代 HTTP 和主控台 Proxy 端點的憑證〉](#)。

# 在 Linux 上安裝 vCloud Director

# 5

您可以透過在一或多個 Linux 伺服器上安裝 vCloud Director 軟體來建立 vCloud Director 伺服器群組。安裝並設定第一個群組成員時會建立一個回應檔，您將使用這個回應檔設定群組的其他成員。

此程序僅適用於全新安裝作業。如果您是要升級現有的 vCloud Director 安裝，請參閱[第 11 章 升級 vCloud Director](#) 和修補 vCloud Director 應用裝置

---

**重要** 不支援在同一個伺服器群組中的 Linux 和 vCloud Director 應用裝置部署上混合安裝 vCloud Director。

---

## 必要條件

- 確認伺服器群組的目標伺服器符合[第 2 章 vCloud Director 硬體及軟體需求](#)。
- 確認已為伺服器群組之目標伺服器的每個端點建立 SSL 憑證。SSL 憑證路徑名稱中的所有目錄必須可供任何使用者讀取。在伺服器群組的所有成員上使用相同的金鑰儲存區路徑可簡化安裝程序，例如 `/tmp/certificates.ks`。請參閱[為 Linux 上的 vCloud Director 建立 SSL 憑證之前](#)。
- 確認已準備好 vCloud Director 伺服器群組的所有目標伺服器都可以存取的 NFS 或其他共用儲存磁碟區。請參閱[準備傳輸伺服器儲存區](#)。
- 確認已建立 vCloud Director 資料庫，且該資料庫可供群組中的所有伺服器存取。請參閱[準備 vCloud Director 資料庫](#)。確認資料庫伺服器重新開機時資料庫服務會啟動。
- 確認所有 vCloud Director 伺服器、資料庫伺服器、所有 vCenter Server 系統和相關聯的 NSX Manager 執行個體可以依照 [vCloud Director 的網路組態需求](#) 中所述解析環境中的每個主機名稱。
- 確認所有 vCloud Director 伺服器與資料庫伺服器是否已與網路時間伺服器同步化，公差註明如下 [vCloud Director 的網路組態需求](#)。
- 如果您計劃從 LDAP 服務匯入使用者或群組，請確認該服務是否可供每個 vCloud Director 伺服器存取。
- 開啟防火牆連接埠，方法如[網路安全性需求](#)所示。連接埠 443 在 vCloud Director 與 vCenter Server 系統間必須為開啟狀態。

## 程序

### 1 在伺服器群組的第一個成員上安裝 vCloud Director 軟體

準備好環境，並確認先決條件後，您可以開始在第一個目標 Linux 伺服器上執行 vCloud Director 安裝程式以建立 vCloud Director 伺服器群組。

## 2 設定網路與資料庫連線

在伺服器群組的第一個成員上安裝 vCloud Director 後，您必須執行組態指令碼，以針對此儲存格建立網路與資料庫連線。此指令碼會建立一個回應檔，當您設定伺服器群組的其他成員時必須使用此回應檔。

## 3 在伺服器群組的其他成員上安裝 vCloud Director

您可以隨時新增伺服器至 vCloud Director 伺服器群組。由於伺服器群組中的所有伺服器都必須以相同的資料庫連線詳細資料來設定，因此您必須使用設定群組的第一個成員時所建立的回應檔。

## 4 設定 vCloud Director

安裝並設定 vCloud Director 伺服器群組中的所有伺服器後，您必須設定 vCloud Director 安裝。vCloud Director 設定會使用授權金鑰、系統管理員帳戶和相關資訊來初始化 vCloud Director 資料庫。

### 後續步驟

您可以開始將資源新增至 vCloud Director 安裝。若要開始使用 vCloud Director，請參閱《vCloud Director 管理員指南》。

## 在伺服器群組的第一個成員上安裝 vCloud Director 軟體

準備好環境，並確認先決條件後，您可以開始在第一個目標 Linux 伺服器上執行 vCloud Director 安裝程式以建立 vCloud Director 伺服器群組。

vCloud Director for Linux 是以數位簽署的可執行檔形式來散佈，名稱採用 `vmware-vcloud-director-distribution-v` 形式。`v.v.nnnnnn.bin` 格式，其中 `v.v.v` 代表產品版本，`nnnnnn` 代表組建編號。例如：`vmware-vcloud-director-distribution-8.10.0-3698331.bin`。執行此可執行檔可安裝或升級 vCloud Director。

vCloud Director 安裝程式會驗證目標伺服器是否符合所有平台先決條件，並在其上安裝 vCloud Director 軟體。

### 必要條件

- 驗證您是否具有目標伺服器的 Superuser 認證。
- 如果想要安裝程式驗證安裝檔案的數位簽章，請在目標伺服器上下載並安裝 VMware 公開金鑰。如果已驗證安裝檔案的數位簽章，則在安裝期間不需要再次驗證它。請參閱[下載並安裝 VMware 公用金鑰](#)。

### 程序

- 1 以根使用者身分登入目標伺服器。
- 2 將安裝檔案下載至目標伺服器。

如果已購買媒體上的軟體，請將安裝檔案複製到目標伺服器可以存取的位置。

### 3 驗證下載的總和檢查碼是否符合下載頁面上公佈的總和檢查碼。

MD5 及 SHA1 總和檢查碼的值會公佈在下載頁面上。請使用適當的工具，驗證已下載的安裝檔案的總和檢查碼是否符合下載頁面上顯示的總和檢查碼。下列格式的 Linux 命令會顯示 *installation-file* 的總和檢查碼。

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

此命令會傳回必須符合下載頁面上的 MD5 總和檢查碼的安裝檔案總和檢查碼。

### 4 確定安裝檔案可以執行。

安裝檔案需要執行權限。若要確定它具有此權限，請開啟主控台、Shell 或終端機視窗，並執行下列 Linux 命令，其中 *installation-file* 是 vCloud Director 安裝檔案的完整路徑名稱。

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

### 5 執行安裝檔案。

若要執行安裝檔案，請輸入其完整路徑名稱，例如：

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

此檔案包括安裝指令碼及內嵌式 RPM 套件。

---

**備註** 無法從路徑名稱內含任何空格字元的目錄執行安裝檔案。

---

如果未在目標伺服器上安裝 VMware 公開金鑰，安裝程式便會顯示下列格式的警告：

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

安裝程式會執行下列動作。

- a 確認主機符合所有需求。
- b 確認安裝檔案的數位簽章。
- c 建立 vcloud 使用者和群組。
- d 解壓縮 vCloud Director RPM 套件。
- e 安裝軟體。

安裝完成時，安裝程式會提示您執行組態指令碼，來設定網路及資料庫連線。

### 6 選取是否執行組態指令碼。

- a 若要在互動模式中執行組態指令碼，請輸入 **y** 並按 Enter 鍵。
- b 若稍後要在互動模式或自動模式下執行組態指令碼，請輸入 **n** 並按 Enter 鍵。

## 設定網路與資料庫連線

在伺服器群組的第一個成員上安裝 vCloud Director 後，您必須執行組態指令碼，以針對此儲存格建立網路與資料庫連線。此指令碼會建立一個回應檔，當您設定伺服器群組的其他成員時必須使用此回應檔。

vCloud Director 伺服器群組的所有成員會共用資料庫連線和其他組態詳細資料。在 vCloud Director 伺服器群組的第一個成員上執行組態指令碼時，該指令碼會建立一個回應檔，該檔案會保留資料庫連線資訊以供後續伺服器安裝使用。

您可以在互動模式或自動模式中執行組態指令碼。對於互動式組態，請執行沒有選項的命令，指令碼會提示您輸入所需的設定資訊。對於自動組態，可透過使用命令選項提供設定資訊。

如果您想要使用具有兩個不同連接埠 (用於 HTTP 服務和主控台 Proxy 服務) 的單一 IP 位址，則必須在自動模式下執行組態指令碼。

---

**備註** 儲存格管理工具包含可用於變更初始設定的網路及資料庫連線詳細資料的子命令。使用這些子命令做出的變更會寫入全域組態檔和回應檔。如需使用儲存格管理工具的相關資訊，請參閱《vCloud Director 管理員指南》。

---

### 必要條件

- 對於互動式組態，請檢閱 [互動式組態參考](#)。
- 對於自動組態，請檢閱 [自動組態參考](#)。
- 執行自動組態之前，請確認環境變數 VCLLOUD\_HOME 的值是否設為安裝 vCloud Director 所在目錄的完整路徑名稱。此值通常為 `/opt/vmware/vcloud-director`。

### 程序

- 1 以根使用者身分登入 vCloud Director 伺服器。
- 2 執行 `configure` 命令：
  - 對於互動模式，請執行命令，並在出現提示時提供所需的資訊。

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

- 對於自動模式，請執行具有選項和引數的命令。

```
/opt/vmware/vcloud-director/bin/configureoptions -unattended
```

指令碼會驗證資訊，然後：

- a 初始化資料庫並將伺服器與其連線。
  - b 顯示 vCloud Director 服務啟動後可用於連線至 **VMware vCloud Director 設定精靈** 的 URL。
  - c 啟動 vCloud Director 儲存格。
- 3 (選擇性) 記下 **VMware vCloud Director 設定精靈** URL，並輸入 `y` 以啟動 vCloud Director 服務。  
您可以透過執行 `service vmware-vcd start` 命令稍後啟動服務。

## 結果

資料庫連線資訊與其他您在設定期間提供的可重複使用的資訊都保留在此伺服器上 `/opt/vmware/vcloud-director/etc/responses.properties` 的回應檔中。此檔案包含機密資訊，在您新增伺服器到伺服器群組時將會再用到。

## 後續步驟

將回應檔的複本儲存在安全的位置。限制它的存取，並確定已將它備份至安全的位置。備份檔案時，請避免透過公用網路傳送純文字。

如果您計劃將伺服器新增至伺服器群組，請將共用傳輸儲存區掛接到 `/opt/vmware/vcloud-director/data/transfer`。

## 互動式組態參考

在互動模式下執行 `configure` 指令碼時，該指令碼會提示您輸入下列資訊。

若要接受預設值，請按 Enter 鍵。

表 5-1. 互動式網路及資料庫設定期間所需的資訊

必要資訊	說明
HTTP 服務的 IP 位址	預設為第一個可用的 IP 位址。
主控台 Proxy 服務的 IP 位址	預設為第一個可用的 IP 位址。
	<b>備註</b> 如果您想要使用具有兩個不同連接埠 (用於 HTTP 服務和主控台 Proxy 服務) 的單一 IP 位址，則必須在自動模式下執行組態指令碼。
Java 金鑰儲存區檔案的完整路徑	例如 <code>/opt/keystore/certificates.ks</code> 。
金鑰儲存區的密碼	請參閱為 <a href="#">Linux 上的 vCloud Director 建立 SSL 憑證之前</a> 。
HTTP SSL 憑證的私密金鑰密碼	請參閱為 <a href="#">Linux 上的 vCloud Director 建立 SSL 憑證之前</a> 。
主控台 Proxy SSL 憑證的私密金鑰密碼	請參閱為 <a href="#">Linux 上的 vCloud Director 建立 SSL 憑證之前</a> 。
啟用遠端稽核記錄到 Syslog 主機	每個 vCloud Director 儲存格中的服務會將稽核訊息記錄到 vCloud Director 資料庫，並在 90 天後到期。若要延長稽核訊息到期時限，請設定 vCloud Director 服務將稽核訊息傳送到 <code>syslog</code> 公用程式 (仍同時傳送到 vCloud Director 資料庫)。 <ul style="list-style-type: none"> <li>■ 若要略過，請按 Enter 鍵。</li> <li>■ 若要啟用，請輸入 Syslog 主機名稱或 IP 位址。</li> </ul>
如果已啟用遠端稽核記錄，則需要 Syslog 主機的 UDP 連接埠	預設為 514。
資料庫類型	PostgreSQL 或 Microsoft SQL Server。 預設為 PostgreSQL。
資料庫伺服器的主機名稱或 IP 位址	執行資料庫的伺服器。

表 5-1. 互動式網路及資料庫設定期間所需的資訊 (續)

必要資訊	說明
資料庫連接埠	對於 PostgreSQL，預設為 5432。 對於 Microsoft SQL Server，預設為 1433。
資料庫名稱	預設為 vcloud。
如果資料庫類型為 Microsoft SQL Server，則為資料庫執行個體	預設為預設執行個體。
資料庫使用者名稱	請參閱準備 vCloud Director 資料庫。
資料庫密碼	請參閱準備 vCloud Director 資料庫。
加入或不參與 VMware 客戶經驗改進計劃 (CEIP)	此產品參與 VMware 客戶經驗改進計劃 (「CEIP」)。 關於透過 CEIP 收集的資料以及 VMware 使用這些資料之用途的詳細資料載於信任與保證中心，網址為 <a href="http://www.vmware.com/trustvmware/ceip.html">http://www.vmware.com/trustvmware/ceip.html</a> 。您可以使用儲存格管理工具隨時加入或退出此產品的 VMware CEIP。請參閱《vCloud Director 管理員指南》中的〈儲存格管理工具參考〉。 若要加入此計劃，請輸入 <b>y</b> 。 如果您不想參與 VMware CEIP 計劃，請輸入 <b>n</b> 。

## 自動組態參考

在自動模式下執行 `configure` 指令碼時，您可以在命令列中提供設定資訊作為選項和參數。

表 5-2. 組態公用程式選項和引數

選項	引數	描述
<code>--help(-h)</code>	無	顯示組態選項和引數的摘要
<code>--config-file (-c)</code>	<code>global.properties</code> 檔案的路徑	您在執行組態公用程式時提供的資訊會儲存在此檔案中。如果省略此選項，則預設位置為 <code>/opt/vmware/vcloud-director/etc/global.properties</code> 。
<code>--console-proxy-ip (-cons)</code>	IPv4 位址，連接埠號碼為選擇性	系統會將此位址用於 vCloud Director 主控台 Proxy 服務。例如， <code>10.17.118.159</code> 。
<code>--console-proxy-port-https</code>	0-65535 範圍內的整數	用於 vCloud Director 主控台 Proxy 服務的連接埠號碼。
<code>--database-ssl</code>	<code>true</code> 或 <code>false</code>	如果您使用的是 PostgreSQL 資料庫，則可以將資料庫設定為需要來自 vCloud Director 的良好簽署的 SSL 連線。如果 <code>--database-type</code> 不是 <code>postgres</code> ，請忽略。 如果您要將 PostgreSQL 資料庫設定為使用自我簽署憑證或私密憑證，請參閱在外部 PostgreSQL 資料庫上執行其他組態。

表 5-2. 組態公用程式選項和引數 (續)

選項	引數	描述
--database-host(-dbhost)	vCloud Director 資料庫主機的 IP 位址或完整網域名稱	請參閱準備 vCloud Director 資料庫。
--database-domain(-dbdomain)	SQL Server 資料庫使用者網域	如果 --database-type 是 sqlserver, 則為選擇性。
--database-instance (-dbinstance)	SQL Server 資料庫執行個體	如果 --database-type 是 sqlserver, 則加以使用。
--database-name (-dbname)	資料庫服務名稱	請參閱準備 vCloud Director 資料庫。
--database-password (-dbpassword)	資料庫使用者的密碼。它可以為 Null。	請參閱準備 vCloud Director 資料庫。
--database-port (-dbport)	資料庫服務在資料庫主機上使用的連接埠號碼	請參閱準備 vCloud Director 資料庫。
--database-type (-dbtype)	資料庫類型。可以為: ■ postgres ■ sqlserver	請參閱準備 vCloud Director 資料庫。
--database-user (-dbuser)	資料庫使用者的使用者名稱。	請參閱準備 vCloud Director 資料庫。
--enable-ceip	true 或 false	此產品參與 VMware 客戶經驗改進計劃 (「CEIP」)。關於透過 CEIP 收集的資料以及 VMware 使用這些資料之用途的詳細資料載於信任與保證中心, 網址為 <a href="http://www.vmware.com/trustvmware/ceip.html">http://www.vmware.com/trustvmware/ceip.html</a> 。您可以使用儲存格管理工具隨時加入或退出此產品的 VMware CEIP。請參閱《vCloud Director 管理員指南》中的〈儲存格管理工具參考〉。
--uuid (-g)	無	為儲存格產生新的唯一識別碼
--primary-ip (-ip)	IPv4 位址, 連接埠號碼為選擇性	系統會將此位址用於 vCloud Director Web 介面服務。例如, 10.17.118.159。
--primary-port-http	0 到 65535 範圍內的整數	用於與 vCloud Director Web 介面服務建立 HTTP (不安全) 連線的連接埠號碼
--primary-port-https	0-65535 範圍內的整數	用於與 vCloud Director Web 介面服務建立 HTTPS (安全) 連線的連接埠號碼
--keystore (-k)	包含 SSL 憑證和私密金鑰的 Java 金鑰儲存區路徑	必須是完整路徑名稱。例如 /opt/keystore/certificates.ks。

表 5-2. 組態公用程式選項和引數 (續)

選項	引數	描述
<code>--syslog-host (-loghost)</code>	Syslog 伺服器主機的 IP 位址或完整網域名稱	每個 vCloud Director 儲存格中的服務會將稽核訊息記錄到 vCloud Director 資料庫，並在 90 天後到期。若要延長稽核訊息到期時限，請設定 vCloud Director 服務將稽核訊息傳送到 <code>syslog</code> 公用程式(仍同時傳送到 vCloud Director 資料庫)。
<code>--syslog-port (-logport)</code>	0-65535 範圍內的整數	<code>syslog</code> 程序所在連接埠，以便該程序監視指定的伺服器。若未指定，則預設為 514。
<code>--response-file (-r)</code>	回應檔案的路徑	必須是完整路徑名稱。若未指定，則預設為 <code>/opt/vmware/vcloud-director/etc/responses.properties</code> 。您在執行設定時提供的所有資訊均會保留在此檔案中。  <b>重要</b> 此檔案包含機密資訊，在您新增伺服器到伺服器群組時將會用到。將檔案保留存在安全的位置，且僅在需要時才提供使用。
<code>--unattended-installation (-unattended)</code>	無	指定自動安裝
<code>--keystore-password (-w)</code>	SSL 憑證金鑰儲存區密碼	SSL 憑證金鑰儲存區密碼。

### 範例：具有兩個 IP 位址的自動組態

下列範例命令針對具有兩個不同 IP 位址 (用於 HTTP 服務和主控台 Proxy 服務) 的 vCloud Director 伺服器執行自動組態。

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./configure -ip 10.17.118.159 -cons 10.17.118.158 \
-dbtype sqlserver -dbhost 10.150.10.78 -dbname mssql-db -dbuser vcloud --enable-ceip true \
-dbpassword P@55word -k /opt/keystore/certificates.ks -w $3Cret -loghost 10.150.10.10 -unattended
```

### 範例：具有單一 IP 位址的自動組態

下列範例命令針對具有單一 IP 位址 (具有兩個連接埠，分別用於 HTTP 服務和主控台 Proxy 服務) 的 vCloud Director 伺服器執行自動組態。

```
[root@cell1 /opt/vmware/vcloud-director/
bin]# ./configure -ip 10.17.118.159 --primary-port-https 9000 -cons 10.17.118.159 \
--console-proxy-port-https 9010 -dbtype sqlserver -dbhost 10.150.10.78 -dbname mssql-db \
-dbuser vcloud -dbpassword P@55word -k /opt/keystore/certificates.ks -w $3Cret \
-loghost 10.150.10.10 --enable-ceip true -unattended
```

## 保護和重複使用回應檔

對第一個 vCloud Director 儲存格設定的網路及資料庫連線詳細資料會儲存在回應檔中。此檔案包含機密資訊，在您新增伺服器到伺服器群組時將會再用到。您必須將檔案保存在安全的位置。

回應檔建立在第一個資料庫上的 `/opt/vmware/vcloud-director/etc/responses.properties`，供您設定網路及資料庫連線。新增更多伺服器至群組時，您必須使用回應檔的複本，以提供所有伺服器共用的組態參數。

---

**重要** 儲存格管理工具包含可用於變更初始指定的網路及資料庫連線詳細資料的子命令。使用這些工具做出的變更會寫入全域組態檔和回應檔，因此在使用任何可修改回應檔的命令前，請務必確定回應檔已存在 (位於 `/opt/vmware/vcloud-director/etc/responses.properties`) 並且可寫入。

---

### 程序

#### 1 保護回應檔。

將檔案的複本儲存在安全的位置。限制它的存取，並確定已將它備份至安全的位置。備份檔案時，請避免透過公用網路傳送純文字。

#### 2 重複使用回應檔。

a 將檔案複製至您準備要設定的伺服器可以存取的位置。

---

**備註** 您必須先在伺服器上安裝 vCloud Director 軟體後，才可以重複使用回應檔來設定軟體。回應檔路徑名稱中的所有目錄必須可供使用者 `vcloud.vcloud` 讀取，如此範例所示。

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

安裝程式會建立此使用者和群組。

b 使用 `-r` 選項並指定回應檔路徑名稱來執行組態指令碼。

以根使用者身分登入，開啟主控台、Shell 或是終端機視窗，然後輸入：

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

### 後續步驟

設定其他伺服器之後，請刪除您用來設定它們的回應檔複本。

## 在伺服器群組的其他成員上安裝 vCloud Director

您可以隨時新增伺服器至 vCloud Director 伺服器群組。由於伺服器群組中的所有伺服器都必須以相同的資料庫連線詳細資料來設定，因此您必須使用設定群組的第一個成員時所建立的回應檔。

---

**重要** 不支援在同一個伺服器群組中的 Linux 和 vCloud Director 應用裝置部署上混合安裝 vCloud Director。

---

**必要條件**

- 確認您可以存取設定此伺服器群組的第一個成員時所建立的回應檔。請參閱[設定網路與資料庫連線](#)。
- 確認在 vCloud Director 伺服器群組的第一個成員上掛接了共用傳輸儲存區到 `/opt/vmware/vcloud-director/data/transfer`。

**程序**

- 1 以**根使用者**身分登入目標伺服器。
- 2 將安裝檔案下載至目標伺服器。

如果已購買媒體上的軟體，請將安裝檔案複製到目標伺服器可以存取的位置。

- 3 確定安裝檔案可以執行。

安裝檔案需要執行權限。若要確定它具有此權限，請開啟主控台、Shell 或終端機視窗，並執行下列 Linux 命令，其中 *installation-file* 是 vCloud Director 安裝檔案的完整路徑名稱。

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

- 4 執行安裝檔案。

若要執行安裝檔案，請輸入其完整路徑名稱，例如：

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

此檔案包括安裝指令碼及內嵌式 RPM 套件。

---

**備註** 無法從路徑名稱內含任何空格字元的目錄執行安裝檔案。

---

如果未在目標伺服器上安裝 VMware 公開金鑰，安裝程式便會顯示下列格式的警告：

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

安裝程式會執行下列動作。

- a 確認主機符合所有需求。
- b 確認安裝檔案的數位簽章。
- c 建立 vcloud 使用者和群組。
- d 解壓縮 vCloud Director RPM 套件。
- e 安裝軟體。

安裝完成時，安裝程式會提示您執行組態指令碼，來設定網路及資料庫連線。

- 5 輸入 **n** 並按 Enter 鍵，以拒絕執行組態指令碼。  
可以稍後透過提供回應檔做為輸入，來執行組態指令碼。
- 6 將共用傳輸儲存區掛接到 `/opt/vmware/vcloud-director/data/transfer`。  
伺服器群組中的所有 vCloud Director 伺服器都必須將此磁碟區掛接到同一個掛接點。

## 7 將回應檔複製至此伺服器可存取的位置。

回應檔路徑名稱中的所有目錄必須可供根使用者讀取。

## 8 執行組態指令碼。

- a 透過提供回應檔路徑名稱，來執行 `configure` 命令。

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

該指令碼會將回應檔複製到 `vcloud.vcloud` 能讀取的位置，然後使用回應檔做為輸入，來執行組態指令碼。

- b 出現提示時，提供 HTTP 服務和主控台 Proxy 服務的 IP 位址。
- c 如果出現提示時組態指令碼在儲存於回應檔的路徑名稱中找不到有效憑證，請提供憑證的路徑名稱和密碼。

該指令碼會驗證相關資訊，並會將伺服器連線至資料庫，然後啟動 vCloud Director 儲存格。

## 9 (選擇性) 輸入 `y`，以啟動 vCloud Director 服務。

您可以決定透過執行 `service vmware-vcd start` 命令稍後啟動服務。

### 後續步驟

重複此程序，將更多伺服器新增至此伺服器群組。

在 vCloud Director 服務於所有伺服器上執行時，您必須使用授權金鑰、系統管理員帳戶和相關資訊來初始化 vCloud Director 資料庫。您可以透過下列其中一種方式初始化資料庫：

- 使用網頁瀏覽器，透過組態指令碼完成時顯示的 URL 開啟安裝精靈。請參閱[設定 vCloud Director](#)。
- 將儲存格管理工具與 `system-setup` 子命令搭配使用。如需有關使用儲存格管理工具的資訊，請參閱《vCloud Director 管理員指南》。

## 設定 vCloud Director

安裝並設定 vCloud Director 伺服器群組中的所有伺服器後，您必須設定 vCloud Director 安裝。vCloud Director 設定會使用授權金鑰、系統管理員帳戶和相關資訊來初始化 vCloud Director 資料庫。

執行用於收集 Web 主控台啟動所需的資訊的 **VMware vCloud Director 設定精靈**後，才能啟動 vCloud Director Web 主控台。

除了使用 **VMware vCloud Director 設定精靈**來設定 vCloud Director 安裝，您也可以使用儲存格管理工具的 `system-setup` 子命令。如需儲存格管理工具的相關資訊，請參閱《vCloud Director 管理員指南》。

### 必要條件

- 確認已在所有伺服器上啟動 vCloud Director 服務。

- 從 VMware 授權入口網站取得 vCloud Director 產品序號。

## 程序

### 程序

- 1 開啟網頁瀏覽器並移至組態指令碼顯示的 URL。

若要探索 **VMware vCloud Director 設定精靈** 的 URL，您也可以查詢與您在安裝第一個伺服器時為 HTTP 服務指定的 IP 位址相關聯的完整網域名稱。若要連線至精靈，請移至 <https://fully-qualified-domain-name>，例如 <https://mycloud.example.com>。

---

**備註** 啟動精靈可能需要幾分鐘的時間。

---

- 2 檢閱 [歡迎] 頁面，然後按下一步。
- 3 閱讀並接受授權合約，然後按下一步。  
如果拒絕授權合約，您無法繼續設定 vCloud Director。
- 4 輸入您的 vCloud Director 產品序號，然後按下一步。
- 5 輸入 vCloud Director 系統管理員的使用者名稱、密碼與連絡資訊，然後按下一步。  
vCloud Director 系統管理員在整個雲端擁有 Superuser 權限。此系統管理員可以建立其他系統管理員帳戶。
- 6 設定可控制 vCloud Director 如何與 vSphere 以及 NSX Manager 互動的系統設定，然後按下一步。
  - a 在**系統名稱**文字方塊中，輸入要用於此 vCloud Director 安裝的 vCenter Server 資料夾的名稱。
  - b 在**安裝 ID**文字方塊中，設定此 vCloud Director 安裝的識別碼，以便在為虛擬 NIC 建立 MAC 位址時使用。  
如果您計劃在多站台部署中跨越 vCloud Director 安裝建立延伸網路，請考慮對每個 vCloud Director 安裝設定唯一的安裝識別碼。
- 7 在 [即將登入] 頁面上，檢閱設定並按一下**完成**。

### 結果

設定程序完成後，系統會將您重新導向至 vCloud DirectorWeb 主控台登入頁面。

### 後續步驟

使用系統管理員的使用者名稱和密碼登入 vCloud DirectorWeb 主控台，然後開始佈建您的雲端。如需將資源新增至 vCloud Director 的相關資訊，請參閱《vCloud Director 管理員指南》。

# 部署 vCloud Director 應用裝置

# 6

您可以透過部署 vCloud Director 應用裝置的一或多個執行個體來建立 vCloud Director 伺服器群組。您可以使用 vSphere Client (HTML5)、vSphere Web Client (Flex) 或 VMware OVF Tool 部署 vCloud Director 應用裝置。

---

**重要** 不支援在同一個伺服器群組中的 Linux 和 vCloud Director 應用裝置部署上混合安裝 vCloud Director。

---

vCloud Director 應用裝置是預先設定的虛擬機器，已針對執行 vCloud Director 服務進行最佳化。

散佈應用裝置時使用的名稱形式為 VMware vCloud Director-v.v.v.v-nnnnnn\_OVF10.ova，其中 v.v.v.v 代表產品版本，nnnnnn 代表組建編號。例如：VMware vCloud Director-9.7.0.0-9229800\_OVA10.ova。

vCloud Director 應用裝置套件包含下列軟體：

- VMware Photon™ 作業系統
- vCloud Director 的服務群組
- PostgreSQL 10

主要小型和待命小型 vCloud Director 應用裝置大小適用於實驗室或測試系統。主要大型和待命大型大小符合生產系統的最低大小需求。視工作負載而定，您可能需要新增其他資源。

---

**重要** 不支援在 vCloud Director 應用裝置上安裝任何第三方元件。根據《[VMware 產品互通性對照表](#)》，您只能安裝支援的 VMware 元件。例如，您可以安裝支援的 VMware vRealize® Operations Manager™ 或 VMware vRealize® Log Insight™ 監控代理程式版本。

---

## 應用裝置資料庫組態

從 9.7 版開始，vCloud Director 應用裝置包含具有高可用性 (HA) 功能的內嵌式 PostgreSQL 資料庫。若要建立具有資料庫 HA 叢集的應用裝置部署，您必須將 vCloud Director 應用裝置的一個執行個體部署為主要儲存格，並將此應用裝置的兩個執行個體部署為待命儲存格。您可以將伺服器群組中的其他 vCloud Director 應用裝置執行個體部署為 vCD 應用程式儲存格，以便僅執行不含內嵌式資料庫之 vCloud Director 服務群組。vCD 應用程式儲存格會連線至主要儲存格中的資料庫。請參閱 [應用裝置部署和資料庫高可用性組態](#)。

依預設，vCloud Director 應用裝置會使用 TLS (取代已過時的 SSL) 進行資料庫連線 (包括複寫)。此功能在部署後立即生效，並使用自我簽署的 PostgreSQL 憑證。若要使用來自憑證授權機構 (CA) 的簽署憑證，請參閱[取代自我簽署的內嵌式 PostgreSQL 和 vCloud Director 應用裝置管理 UI 憑證](#)。

---

**備註** vCloud Director 應用裝置不支援外部資料庫。

---

## 應用裝置網路組態

從 9.7 版開始，vCloud Director 應用裝置會部署有兩個網路 `eth0` 和 `eth1`，以便您可以將 HTTP 流量與資料庫流量相互隔離。不同的服務在一或兩個對應網路介面上進行接聽。

服務	eth0 上的連接埠	eth1 上的連接埠
SSH	22	22
HTTP	80	n/a
HTTPS	443	n/a
PostgreSQL	n/a	5432
管理使用者介面	5480	5480
主控台 Proxy	8443	n/a
JMX	8998、8999	n/a
JMS/ActiveMQ	61616	n/a

vCloud Director 應用裝置使用 `iptables` 支援防火牆規則的使用者自訂。若要新增自訂 `iptables` 規則，可以將您自己的組態資料新增至 `/etc/systemd/scripts/iptables` 檔案的結尾。

本章節討論下列主題：

- [應用裝置部署和資料庫高可用性組態](#)
- [部署 vCloud Director 應用裝置的必要條件](#)
- [使用 vSphere Web Client 或 vSphere Client 部署 vCloud Director 應用裝置](#)
- [使用 VMware OVF Tool 部署 vCloud Director 應用裝置](#)

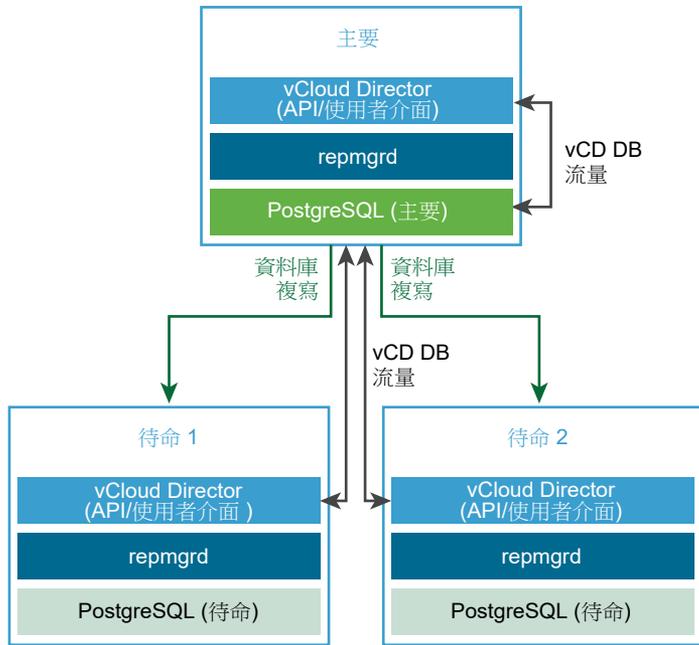
## 應用裝置部署和資料庫高可用性組態

vCloud Director 應用裝置包含內嵌式 PostgreSQL 資料庫。內嵌式 PostgreSQL 資料庫包含 Replication Manager (`repmgr`) 工具套件，可為 PostgreSQL 伺服器叢集提供高可用性 (HA) 功能。您可以建立具有資料庫 HA 叢集的應用裝置部署，以便為 vCloud Director 資料庫提供容錯移轉功能。

您可以將 vCloud Director 應用裝置部署為主要儲存格、待命儲存格或 vCD 應用程式儲存格。請參閱 [使用 vSphere Web Client 或 vSphere Client 部署 vCloud Director 應用裝置](#)、[使用 VMware OVF Tool 部署 vCloud Director 應用裝置](#) 或 [使用已簽署的萬用字元憑證部署 vCloud Director 應用裝置以進行 HTTPS 和主控台 Proxy 通訊](#)。

若要為 vCloud Director 資料庫設定 HA，當您建立伺服器群組時，您可以透過部署 vCloud Director 應用裝置的一個主要執行個體和兩個待命執行個體來設定資料庫 HA 叢集。

圖 6-1. vCloud Director 應用裝置資料庫 HA 叢集



## 建立具有資料庫 HA 的 vCloud Director 應用裝置部署

若要建立具有資料庫 HA 組態的 vCloud Director 伺服器群組，請遵循此工作流程：

- 1 將 vCloud Director 應用裝置部署為主要儲存格。

主要儲存格是 vCloud Director 伺服器群組中的第一個成員。內嵌式資料庫會設定為 vCloud Director 資料庫。資料庫名稱為 `vccloud`，且資料庫使用者為 `vccloud`。

- 2 確認主要儲存格已啟動且正在執行。

- a 若要確認 vCloud Director 服務健全狀況，請使用**系統管理員**認證登入 vCloud Director Web 主控台，網址為 `https://primary_eth0_ip_address/cloud`。
- b 若要確認 PostgreSQL 資料庫健全狀況，請以 **root** 身分登入應用裝置管理使用者介面，網址為 `https://primary_eth1_ip_address:5480`。

主要節點必須處於執行中狀態。

- 3 將兩個 vCloud Director 應用裝置執行個體部署為待命儲存格。

內嵌式資料庫與主要資料庫一起在複寫模式中進行設定。

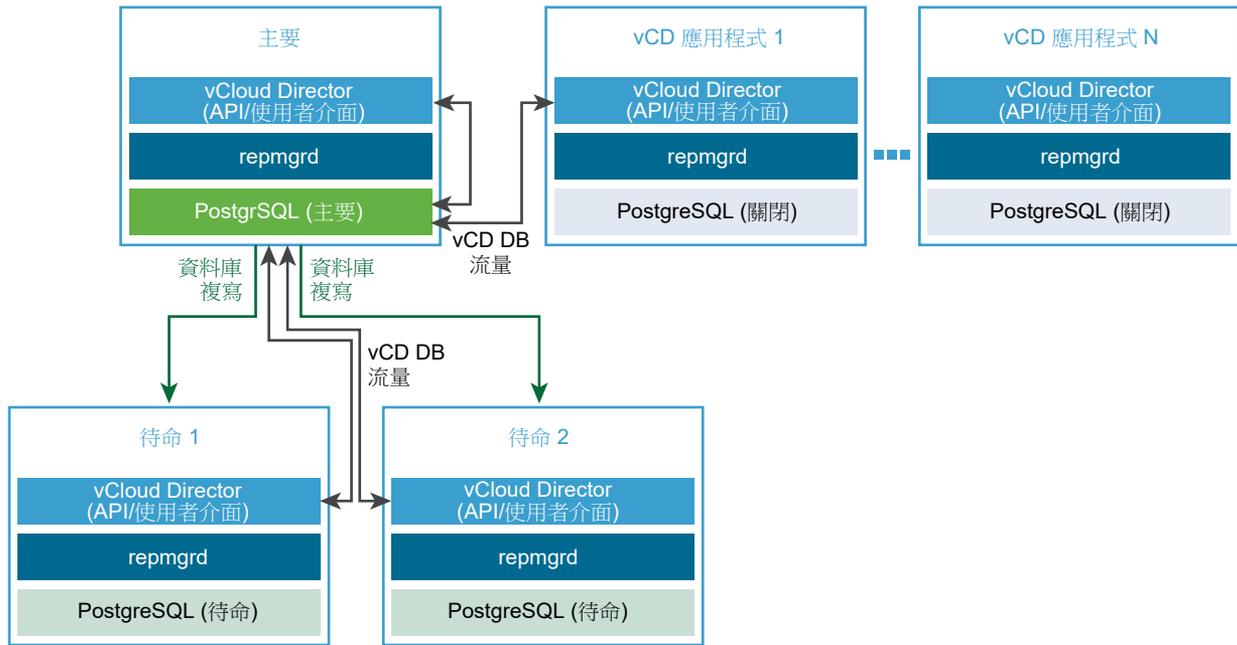
**備註** 初始待命應用裝置部署之後，Replication Manager 開始將其資料庫與主要應用裝置資料庫進行同步。在此期間，vCloud Director 資料庫和 vCloud Director 使用者介面將無法使用。

- 4 確認 HA 叢集中的所有儲存格均在執行中。

請參閱**檢視資料庫高可用性叢集中的儲存格的狀態**。

- 5 (選擇性) 將一或多個 vCloud Director 應用裝置執行個體部署為 vCD 應用程式儲存格。

未使用內嵌式資料庫。vCD 應用程式儲存格會連線至主要資料庫。



## 建立不具有資料庫 HA 的 vCloud Director 應用裝置部署

若要建立不含資料庫 HA 組態的 vCloud Director 伺服器，請遵循此工作流程：

- 1 將 vCloud Director 應用裝置部署為主要儲存格。

主要儲存格是 vCloud Director 伺服器群組中的第一個成員。內嵌式資料庫會設定為 vCloud Director 資料庫。資料庫名稱為 `vccloud`，且資料庫使用者為 `vccloud`。

- 2 確認主要儲存格已啟動且正在執行。

a 若要確認 vCloud Director 服務健全狀況，請使用**系統管理員**認證登入 vCloud Director Web 主控台，網址為 `https://primary_eth0_ip_address/cloud`。

b 若要確認 PostgreSQL 資料庫健全狀況，請以 **root** 身分登入應用裝置管理使用者介面，網址為 `https://primary_eth1_ip_address:5480`。

主要節點必須處於執行中狀態。

- 3 (選擇性) 將一或多個 vCloud Director 應用裝置執行個體部署為 vCD 應用程式儲存格。

未使用內嵌式資料庫。vCD 應用程式儲存格會連線至主要資料庫。



## 部署 vCloud Director 應用裝置的必要條件

若要確保成功部署 vCloud Director 應用裝置，您必須在開始部署前先執行一些工作和預先檢查。

- 確認您擁有 vCloud Director .ova 檔案的存取權。
- 部署主要應用裝置之前，請準備 NFS 共用傳輸服務儲存區。請參閱[準備傳輸伺服器儲存區](#)。

---

**備註** 共用傳輸服務儲存區必須既不包含 responses.properties 檔案，也不包含 appliance-nodes 目錄。

---

- [安裝和設定 RabbitMQ AMQP Broker](#)。

## vCloud Director 應用裝置部署方法

- [使用 vSphere Web Client 或 vSphere Client 部署 vCloud Director 應用裝置](#)
- [使用 VMware OVF Tool 部署 vCloud Director 應用裝置](#)
- [使用已簽署的萬用字元憑證部署 vCloud Director 應用裝置以進行 HTTPS 和主控台 Proxy 通訊](#)

## 使用 vSphere Web Client 或 vSphere Client 部署 vCloud Director 應用裝置

您可以使用 vSphere Web Client (Flex) 或 vSphere Client (HTML5) 將 vCloud Director 應用裝置部署為 OVF 範本。

您必須將 vCloud Director 伺服器群組的第一個成員部署為主要儲存格。您可以將 vCloud Director 伺服器群組的後續成員部署為待命儲存格或 vCD 應用程式儲存格。請參閱[應用裝置部署和資料庫高可用性組態](#)。

---

**重要** 不支援在同一個伺服器群組中的 Linux 和 vCloud Director 應用裝置部署上混合安裝 vCloud Director。

---

如需在 vSphere 中部署 OVF 範本的相關資訊，請參閱《vSphere 虛擬機器管理》。

或者，您可以使用 VMware OVF Tool 部署應用裝置。請參閱[使用 VMware OVF Tool 部署 vCloud Director 應用裝置](#)。

---

**備註** 不支援在 vCloud Director 中部署 vCloud Director 應用裝置。

---

### 必要條件

請參閱[部署 vCloud Director 應用裝置的必要條件](#)。

### 程序

#### 1 啟動 vCloud Director 應用裝置部署

若要啟動應用裝置部署，您可以在 vSphere Web Client (Flex) 或 vSphere Client (HTML5) 中開啟部署精靈。

## 2 自訂 vCloud Director 應用裝置並完成部署

若要設定 vCloud Director 詳細資料，您可以自訂應用裝置範本。

### 後續步驟

- 設定公用主控台 Proxy 位址，因為 vCloud Director 應用裝置將具有自訂連接埠 8443 的 eth0 NIC 用於主控台 Proxy 服務。請參閱[自訂公用端點](#)。
- 若要向 vCloud Director 伺服器群組新增成員，請重複此程序。
- 若要輸入授權金鑰，請登入 vCloud Director Web 主控台。
- 若要取代應用裝置首次開機期間建立的自我簽署憑證，您可以為 [Linux 上的 vCloud Director 建立 CA 簽署的 SSL 憑證金鑰儲存區](#)。

## 啟動 vCloud Director 應用裝置部署

若要啟動應用裝置部署，您可以在 vSphere Web Client (Flex) 或 vSphere Client (HTML5) 中開啟部署精靈。

### 程序

- 1 在 vSphere Web Client 或 vSphere Client 中，在任何詳細目錄物件上按一下滑鼠右鍵，然後按一下 **部署 OVF 範本**。
- 2 輸入 vCloud Director .ova 檔案的路徑，然後按下一步。
- 3 輸入虛擬機器的名稱，並瀏覽 vCenter Server 存放庫以選取要部署應用裝置的資料中心或資料夾，然後按下一步。
- 4 選取您要在其上部署應用裝置的 ESXi 主機或叢集，然後按下一步。
- 5 檢閱範本詳細資料，然後按下一步。
- 6 閱讀並接受授權合約，然後按下一步。
- 7 選取部署類型和大小，然後按下一步。

主要小型和待命小型 vCloud Director 應用裝置大小適用於實驗室或測試系統。主要大型和待命大型大小符合生產系統的最低大小需求。視工作負載而定，您可能需要新增其他資源。

選項	描述
主要小型	將具有 12 GB RAM 和 2 個 vCPU 的應用裝置部署為 vCloud Director 伺服器群組中的第一個成員。 主要儲存格中的內嵌式資料庫設定為 vCloud Director 資料庫。資料庫名稱為 vcloud，且資料庫使用者為 vcloud。
主要大型	將具有 24 GB RAM 和 4 個 vCPU 的應用裝置部署為 vCloud Director 伺服器群組中的第一個成員。 主要儲存格中的內嵌式資料庫設定為 vCloud Director 資料庫。資料庫名稱為 vcloud，且資料庫使用者為 vcloud。

選項	描述
待命小型	用於在資料庫 HA 叢集中加入主要小型儲存格。 將具有 12 GB RAM 和 2 個 vCPU 的應用裝置部署為使用資料庫高可用性組態的 vCloud Director 伺服器群組中的第二個或第三個成員。 待命儲存格中的內嵌式資料庫與主要資料庫一起在複寫模式中進行設定。
待命大型	用於在資料庫 HA 叢集中加入主要大型儲存格。 將具有 24 GB RAM 和 4 個 vCPU 的應用裝置部署為使用資料庫高可用性組態的 vCloud Director 伺服器群組中的第二個或第三個成員。 待命應用裝置中的內嵌式資料庫與主要資料庫一起在複寫模式中進行設定。
vCD 儲存格應用程式	將具有 8 GB RAM 和 2 個 vCPU 的應用裝置部署為 vCloud Director 伺服器群組中的後續成員。 未使用 vCD 應用程式儲存格中的內嵌式資料庫。vCD 應用程式儲存格會連線至主要資料庫。

**重要** vCloud Director 伺服器群組中的主要儲存格和待命儲存格必須大小相同。資料庫 HA 叢集可以由一個主要小型儲存格和兩個待命小型儲存格組成，或由一個主要大型儲存格和兩個待命大型儲存格組成。

部署之後，您可以重新設定應用裝置的大小。

- 為虛擬機器組態檔和虛擬磁碟選取磁碟格式和資料存放區，然後按下一步。  
完整格式可提高效能，而精簡格式可節省儲存空間。
- 從目的地網路儲存格中的下拉式功能表，針對應用裝置的 eth1 和 eth0 NIC 選取目標網路。  
來源網路清單的順序可能相反。確認您為每個來源網路選取了正確的目的地網路。

**重要** 兩個目的地網路必須不同。

- 從 IP 配置設定下拉式功能表中，選取靜態-手動 IP 配置和 IPv4 通訊協定。
- 按下一步。

系統會將您重新導向至自訂範本頁面，以設定 vCloud Director 詳細資料。

## 自訂 vCloud Director 應用裝置並完成部署

若要設定 vCloud Director 詳細資料，您可以自訂應用裝置範本。

自訂 vCloud Director 應用裝置時，您可以設定應用裝置設定、資料庫和網路內容。僅在部署主要應用裝置時設定初始系統設定，此應用裝置是伺服器群組的第一個成員。

**備註** 此程序只有 步驟 3 是選擇性的。您必須完成所有其他步驟，才能自訂 vCloud Director 應用裝置。

## 程序

- 1 在 **VCD 應用裝置設定** 區段中，設定應用裝置詳細資料。

設定	描述
<b>NTP 伺服器</b>	要使用的 NTP 伺服器的主機名稱或 IP 位址。
<b>初始根密碼</b>	應用裝置的初始根密碼。必須包含至少 8 個字元，並且其中有一個大寫字元、一個小寫字元、一個數字以及一個特殊字元。  <b>重要</b> 初始 root 密碼會變成金鑰儲存區密碼。叢集部署要求所有儲存格在初始部署期間具有相同的 root 密碼。開機程序完成後，您可以變更任何所需儲存格上的 root 密碼。  <b>備註</b> OVF 部署精靈不會根據密碼條件驗證初始根密碼。
<b>第一次登入後根密碼過期</b>	如果您想要在第一次登入後繼續使用初始密碼，您必須確認初始密碼符合根密碼條件。若要在第一次登入後繼續使用初始根密碼，請取消選取此選項。
<b>啟用 SSH</b>	依預設已停用
<b>傳輸檔案位置的 NFS 掛接</b>	請參閱 <a href="#">準備傳輸伺服器儲存區</a> 。

**備註** 如需變更應用裝置的日期、時間或時區的相關資訊，請參閱 <https://kb.vmware.com/kb/59674>。

- 2 如果您要部署伺服器群組的第一個成員，請在 **VCD 設定 - 僅「主要」應用裝置需要** 區段中輸入資料庫詳細資料，建立 **系統管理員** 帳戶，並設定系統設定。

資料庫名稱為 vcloud，且資料庫使用者為 vcloud。

設定	描述
<b>'vcloud' 使用者的 'vcloud' 資料庫密碼</b>	vcloud 資料庫使用者的密碼。
<b>管理員使用者名稱</b>	系統管理員帳戶的使用者名稱。預設為 administrator。
<b>管理員全名</b>	系統管理員的全名。預設為 vCD Admin。
<b>管理員使用者密碼</b>	系統管理員帳戶的密碼。
<b>管理員電子郵件</b>	系統管理員的電子郵件地址。
<b>系統名稱</b>	為此 vCloud Director 安裝建立的 vCenter Server 資料夾的名稱。預設為 vcd1。
<b>安裝 ID</b>	為虛擬 NIC 建立 MAC 位址時要使用的此 vCloud Director 安裝的識別碼。預設為 1。  如果您計劃在多站點部署中跨越 vCloud Director 安裝建立延伸網路，請考慮對每個 vCloud Director 安裝設定唯一的安裝識別碼。

- 3 (選擇性) 在 **其他網路內容** 區段中，如果您的網路拓撲需要，請輸入 eth0 和 eth1 網路介面的靜態路由，然後按 **下一步**。

如果您想要透過非預設閘道路由連線到主機，可能需要提供靜態路由。例如，當預設閘道位於 eth0 上時，管理基礎結構僅可透過 eth1 介面進行存取。在大多數情況下，此設定會保留空白。

靜態路由必須是以逗號分隔的路由規格的清單。路由規格必須包含目標開道的 IP 位址和無類別網域間路由選擇 (CIDR) 網路規格 (後者可選)。例如，

**172.16.100.253 172.16.100.0/19, 172.16.100.253 192.168.100.0/24。**

- 在**網路內容**區段中，輸入 eth0 和 eth1 NIC 的網路詳細資料，然後按**下一步**。

**備註** 所有設定都是必要的。

設定	描述
預設開道	應用裝置的預設開道的 IP 位址。
網域名稱	網域名稱，例如 <i>mydomain.com</i> 。
網域搜尋路徑	以逗號或空格分隔的應用裝置網域搜尋路徑的網域名稱清單。
網域名稱伺服器	應用裝置的網域名稱伺服器的 IP 位址。
eth0 網路 IP 位址	eth0 介面的 IP 位址。
eth0 網路遮罩	eth0 介面的網路遮罩或首碼。
eth1 網路 IP 位址	eth1 介面的 IP 位址。
eth1 網路遮罩	eth1 介面的網路遮罩或首碼。

- 在**即將完成**頁面上，檢閱 vCloud Director 應用裝置的組態設定，然後按一下**完成**即可開始部署。

#### 後續步驟

開啟新建立的虛擬機器的電源。

## 使用 VMware OVF Tool 部署 vCloud Director 應用裝置

您可以使用 VMware OVF Tool 將 vCloud Director 應用裝置部署為 OVF 範本。

您必須將 vCloud Director 伺服器群組的第一個成員部署為主要儲存格。您可以將 vCloud Director 伺服器群組的後續成員部署為待命儲存格或 vCD 應用程式儲存格。請參閱 [應用裝置部署和資料庫高可用性組態](#)。

如需安裝 OVF Tool 的相關資訊，請參閱《VMware OVF Tool 版本說明》文件。

如需使用 OVF Tool 的相關資訊，請參閱《OVF Tool 使用者指南》。

執行部署命令之前，請參閱[部署 vCloud Director 應用裝置的必要條件](#)。

部署應用裝置之後，檢視首次開機記錄檔中的警告錯誤訊息。請參閱 [檢查 vCloud Director 應用裝置中的記錄檔](#)。

### 用於部署 vCloud Director 應用裝置的 ovftool 命令選項與內容

選項	值	描述
--noSSLVerify	n/a	略過 vSphere 連線的 SSL 驗證。
--acceptAllEulas	n/a	接受所有使用者授權合約 (EULA)。

選項	值	描述
--datastore	<i>target_vc_datastore</i>	儲存虛擬機器組態檔和虛擬磁碟的目標資料存放區名稱。
--allowAllExtraConfig	n/a	將所有額外的組態選項轉換為 VMX 格式。
--net:"eth0 Network"	<i>portgroup_on_vc_for_eth0</i>	應用裝置 eth0 網路的目的地網路。 <b>重要</b> 必須不同於 eth1 目的地網路。
--net:"eth1 Network"	<i>portgroup_on_vc_for_eth1</i>	應用裝置 eth1 網路的目的地網路。 <b>重要</b> 必須不同於 eth0 目的地網路。
--name	<i>vm_name_on_vc</i>	應用裝置的虛擬機器名稱。
--diskMode	thin 或 thick	虛擬機器組態檔和虛擬磁碟的磁碟格式。
--prop:"vami.ip0.VMware_vCloud_Director" <i>eth0_ip_address</i>		eth0 的 IP 位址。用於使用者介面和 API 存取。在此位址上，DNS 反向查閱確定並設定應用裝置的主機名稱。
--prop:"vami.ip1.VMware_vCloud_Director" <i>eth1_ip_address</i>		eth1 的 IP 位址。用於存取內部服務，包括內嵌式 PostgreSQL 資料庫服務。
--prop:"vami.DNS.VMware_vCloud_Director" <i>dns_ip_address</i>		應用裝置的網域名稱伺服器的 IP 位址。
--prop:"vami.domain.VMware_vCloud_Director" <i>domain_name</i>		DNS 搜尋網域。顯示為搜尋路徑中的第一個元素。
--prop:"vami.gateway.VMware_vCloud_Director" <i>gateway_ip_address</i>		應用裝置的預設閘道的 IP 位址。
--prop:"vami.netmask0.VMware_vCloud_Director" <i>netmask</i>		eth0 介面的網路遮罩或首碼。
--prop:"vami.netmask1.VMware_vCloud_Director" <i>netmask</i>		eth1 介面的網路遮罩或首碼。
--prop:"vami.searchpath.VMware_vCloud_Director" <i>list_of_domain_names</i>		應用裝置的網域搜尋路徑。 以逗號或空格分隔的網域名稱清單。
--prop:"vcloudapp.enable_ssh.VMware_vCloud_Director" <i>enable_ssh</i>		啟用或停用對應用裝置的 SSH 根存取。
--prop:"vcloudapp.expire_root_password.VMware_vCloud_Director" <i>enable_or_expire</i>		決定是否在第一次登入後繼續使用初始密碼。
--prop:"vcloudapp.nfs_mount.VMware_vCloud_Director" <i>ip_address:nfs_mount_path</i>		外部 NFS 伺服器的 IP 位址和匯出路徑。 僅用於主要儲存格。
--prop:"vcloudapp.ntp-server.VMware_vCloud_Director" <i>ntp_server_ip_address</i>		時間伺服器的 IP 位址。
--prop:"vcloudapp.varoot-password.VMware_vCloud_Director" <i>varoot_password</i>		應用裝置的初始根密碼。必須包含至少 8 個字元，並且其中有一個大寫字元、一個小寫字元、一個數字以及一個特殊字元。 <b>重要</b> 初始 root 密碼會變成金鑰儲存區密碼。叢集部署要求所有儲存格在初始部署期間具有相同的 root 密碼。開機程序完成後，您可以變更任何所需儲存格上的 root 密碼。
--prop:"vcloudconf.db_pwd.VMware_vCloud_Director" <i>database_password</i>		vcloud 使用者的資料庫密碼。 僅用於主要儲存格。

選項	值	描述
--prop:"vcloudwiz.admin_email.VMware_vCloud_Director_email_address	<code>vcloudwiz.admin_email</code>	系統管理員帳戶的電子郵件地址。 僅用於主要儲存格。
--prop:"vcloudwiz.admin_fname.VMware_vCloud_Director_fname	<code>vcloudwiz.admin_fname</code>	系統管理員帳戶的名稱。 僅用於主要儲存格。
--prop:"vcloudwiz.admin_pwd.VMware_vCloud_Director_password	<code>vcloudwiz.admin_pwd</code>	系統管理員帳戶的密碼。 僅用於主要儲存格。
--prop:"vcloudwiz.admin_uname.VMware_vCloud_Director_username	<code>vcloudwiz.admin_uname</code>	系統管理員帳戶的使用者名稱。 僅用於主要儲存格。
--prop:"vcloudwiz.inst_id.VMware_vCloud_Director_inst_ID	<code>vcloudwiz.inst_id</code>	vCloud Director 安裝識別碼。 僅用於主要儲存格。
--prop:"vcloudconf.sys_name.VMware_vCloud_Director_system_name	<code>vcloudconf.sys_name</code>	為此 vCloud Director 安裝建立的 vCenter Server 資料夾的名稱。
--prop:"vcloudnet.routes0.VMware_vCloud_Director_routes0_cidr, ip_address2, ...	<code>vcloudnet.routes0</code>	選擇性。eth0 介面的靜態路由。必須是以 逗號分隔的路由規格清單。路由規格必須 包含閘道 IP 位址和無類別網域間路由選擇 (CIDR) 網路規格 (首碼/位元) (後者可選)。 例如, <b>172.16.100.253 172.16.100/19,</b> <b>172.16.200.253。</b>
--prop:"vcloudnet.routes1.VMware_vCloud_Director_routes1_cidr, ip_address2, ...	<code>vcloudnet.routes1</code>	選擇性。eth1 介面的靜態路由。必須是以 逗號分隔的路由規格清單。路由規格必須 包含閘道 IP 位址和無類別網域間路由選擇 (CIDR) 網路規格 (首碼/位元) (後者可選)。 例如, <b>172.16.100.253 172.16.100/19,</b> <b>172.16.200.253。</b>

選項	值	描述
<code>--deploymentOption</code>	<code>primary-small</code> 、 <code>primary-large</code> 、 <code>standby-small</code> 、 <code>standby-large</code> 或 <code>cell</code>	<p>您要部署的應用裝置類型和大小。</p> <p>主要小型和待命小型應用裝置大小適用於實驗室或測試系統。主要大型和待命大型大小符合生產系統的最低大小需求。視工作負載而定，您可能需要新增其他資源。</p> <ul style="list-style-type: none"> <li>■ <code>primary-small</code> 將具有 12 GB RAM 和 2 個 vCPU 的應用裝置部署為 vCloud Director 伺服器群組中的第一個成員。主要儲存格中的內嵌式資料庫設定為 vCloud Director 資料庫。資料庫名稱為 <code>vcloud</code>，且資料庫使用者為 <code>vcloud</code>。</li> <li>■ <code>primary-large</code> 將具有 24 GB RAM 和 4 個 vCPU 的應用裝置部署為 vCloud Director 伺服器群組中的第一個成員。主要儲存格中的內嵌式資料庫設定為 vCloud Director 資料庫。資料庫名稱為 <code>vcloud</code>，且資料庫使用者為 <code>vcloud</code>。</li> <li>■ <code>standby-small</code> 將具有 12 GB RAM 和 2 個 vCPU 的應用裝置部署為使用資料庫高可用性組態的 vCloud Director 伺服器群組中的第二個或第三個成員。待命儲存格中的內嵌式資料庫與主要資料庫一起在複寫模式中進行設定。</li> <li>■ <code>standby-large</code> 將具有 24 GB RAM 和 4 個 vCPU 的應用裝置部署為使用資料庫高可用性組態的 vCloud Director 伺服器群組中的第二個或第三個成員。待命儲存格中的內嵌式資料庫與主要資料庫一起在複寫模式中進行設定。</li> <li>■ <code>cell</code> 將具有 8 GB RAM 和 2 個 vCPU 的應用裝置部署為 vCloud Director 伺服器群組中的後續成員。未使用 vCD 應用程式儲存格中的內嵌式資料庫。vCD 應用程式儲存格會連線至主要資料庫。</li> </ul> <p><b>重要</b> vCloud Director 伺服器群組中的主要儲存格和待命儲存格必須大小相同。資料庫 HA 叢集可以由一個主要小型儲存格和兩個待命小型儲存格組成，或由一個主要大型儲存格和兩個待命大型儲存格組成。</p> <p>部署之後，您可以重新設定應用裝置的大小。</p>
<code>--powerOn</code>	<code>path_to_ova</code>	部署後開啟虛擬機器電源。

## 部署主要 vCloud Director 應用裝置的範例命令

```

ovftool \
--noSSLVerify \
--acceptAllEulas \
--datastore='datastore6' \
--allowAllExtraConfig \
--net:"eth0 Network"="My_UI_API_Network" \
--net:"eth1 Network"="My_Internal_DB_Services_Network" \
--name=MyAppliance \
--diskMode=thin \
--prop:"vami.ip0.VMware_vCloud_Director"="10.0.0.142" \
--prop:"vami.ip1.VMware_vCloud_Director"="172.18.41.24" \
--prop:"vami.DNS.VMware_vCloud_Director"="10.0.0.2" \
--prop:"vami.domain.VMware_vCloud_Director"="mycompany.com" \
--prop:"vami.gateway.VMware_vCloud_Director"="10.0.0.1" \
--prop:"vami.netmask0.VMware_vCloud_Director"="255.255.0.0" \
--prop:"vami.netmask1.VMware_vCloud_Director"="255.255.224.0" \
--prop:"vami.searchpath.VMware_vCloud_Director"="eng.mycompany.com" \
--prop:"vcloudapp.enable_ssh.VMware_vCloud_Director"="False" \
--prop:"vcloudapp.expire_root_password.VMware_vCloud_Director"="True" \
--prop:"vcloudapp.nfs_mount.VMware_vCloud_Director"="10.0.0.96:/data/transfer" \
--prop:"vcloudapp.ntp-server.VMware_vCloud_Director"="time.mycompany.com" \
--prop:"vcloudapp.varoot-password.VMware_vCloud_Director"="44z1Bd1HwIt#" \
--prop:"vcloudconf.db_pwd.VMware_vCloud_Director"="Xj052mXAP7n#" \
--prop:"vcloudconf.admin_email.VMware_vCloud_Director"="admin@mycompany.com" \
--prop:"vcloudconf.admin_fname.VMware_vCloud_Director"="vcdadmin" \
--prop:"vcloudconf.admin_pwd.VMware_vCloud_Director"="o@e@vJW26Pnb" \
--prop:"vcloudconf.admin_uname.VMware_vCloud_Director"="administrator" \
--prop:"vcloudconf.inst_id.VMware_vCloud_Director"="59" \
--prop:"vcloudconf.sys_name.VMware_vCloud_Director"="MyAppliance" \
--deploymentOption="primary-small" \
--powerOn "/MyPath/VMware_vCloud_Director-version_number_OVF10.ova" \
vi://vc_user_name:vc_password@vc_hostname_or_ip_address/vc_datacenter_name/host/vc_cluster_name

```

## 部署待命 vCloud Director 應用裝置的範例命令

```

ovftool \
--noSSLVerify \
--acceptAllEulas \
--datastore='datastore6' \
--allowAllExtraConfig \
--net:"eth0 Network"="My_UI_API_Network" \
--net:"eth1 Network"="My_Internal_DB_Services_Network" \
--name=MySecondAppliance \
--diskMode=thin \
--prop:"vami.ip0.VMware_vCloud_Director"="10.0.0.143" \
--prop:"vami.ip1.VMware_vCloud_Director"="172.18.41.25" \
--prop:"vami.DNS.VMware_vCloud_Director"="10.0.0.2" \
--prop:"vami.domain.VMware_vCloud_Director"="mycompany.com" \
--prop:"vami.gateway.VMware_vCloud_Director"="10.0.0.1" \
--prop:"vami.netmask0.VMware_vCloud_Director"="255.255.0.0" \
--prop:"vami.netmask1.VMware_vCloud_Director"="255.255.224.0" \

```

```
--prop:"vami.searchpath.VMware_vCloud_Director"="eng.mycompany.com" \  
--prop:"vcloudapp.enable_ssh.VMware_vCloud_Director"="False" \  
--prop:"vcloudapp.expire_root_password.VMware_vCloud_Director"="True" \  
--prop:"vcloudapp.nfs_mount.VMware_vCloud_Director"="10.0.0.96:/data/transfer" \  
--prop:"vcloudapp.ntp-server.VMware_vCloud_Director"="time.mycompany.com" \  
--prop:"vcloudapp.varoot-password.VMware_vCloud_Director"="44z1Bd1HwIt#" \  
--prop:"vcloudconf.sys_name.VMware_vCloud_Director"="MySecondAppliance" \  
--deploymentOption="standby-small" \  
--powerOn "/MyPath/VMware_vCloud_Director-version_number_OVF10.ova" \  
vi://vc_user_name:vc_password@vc_hostname_or_ip_address/vc_datacenter_name/host/vc_cluster_name
```

# vCloud Director 應用裝置 SSL 憑證 建立和管理

# 7

vCloud Director 應用裝置使用 SSL 保護用戶端與伺服器之間通訊的安全。每個 vCloud Director 應用裝置必須支援兩個不同的 SSL 端點 - 用於 HTTPS 和主控台 Proxy 通訊。

這些端點可以是不同的 IP 位址，或是包含兩個不同連接埠的單一 IP 位址。每個端點均需要其專屬的 SSL 憑證。您可以針對兩個端點使用相同的憑證 (例如萬用字元憑證)。

本章節討論下列主題：

- 使用已簽署的萬用字元憑證部署 vCloud Director 應用裝置以進行 HTTPS 和主控台 Proxy 通訊
- 建立 CA 簽署的 SSL 憑證並將其匯入至 vCloud Director 應用裝置
- 將私密金鑰和 CA 簽署的 SSL 憑證匯入至 vCloud Director 應用裝置
- 取代自我簽署的內嵌式 PostgreSQL 和 vCloud Director 應用裝置管理 UI 憑證
- 更新 vCloud Director 應用裝置憑證

## 使用已簽署的萬用字元憑證部署 vCloud Director 應用裝置以進行 HTTPS 和主控台 Proxy 通訊

您可以使用已簽署的萬用字元憑證部署 vCloud Director 應用裝置。您可以使用這些憑證來保護不限數量的伺服器，這些伺服器是憑證中所列網域名稱的子網域。

依預設，部署 vCloud Director 應用裝置時，vCloud Director 會產生自我簽署憑證，並使用這些憑證來設定用於 HTTPS 和主控台 Proxy 通訊的 vCloud Director 儲存格。

當您成功部署主要應用裝置時，應用裝置組態邏輯會將 `responses.properties` 檔案從主要應用裝置複製到通用 NFS 共用傳輸服務儲存區 (位於 `/opt/vmware/vcloud-director/data/transfer`)。為此 vCloud Director 伺服器群組部署的其他應用裝置將會使用此檔案自動進行設定。

`responses.properties` 檔案包含 SSL 憑證金鑰儲存區的路徑，其中包含自動產生的自我簽署憑證 `user.keystore.path`。依預設，此路徑指向每個應用裝置的本機金鑰儲存區檔案。

部署主要應用裝置後，您可以將其重新設定為使用已簽署的憑證。如需有關使用已簽署憑證建立金鑰儲存區的詳細資訊，請參閱[建立 CA 簽署的 SSL 憑證並將其匯入至 vCloud Director 應用裝置](#)。

如果您在主要 vCloud Director 應用裝置上使用的已簽署憑證是簽署的萬用字元憑證，則這些憑證可套用至 vCloud Director 伺服器群組中的所有其他應用裝置，即待命儲存格和 vCloud Director 應用程式儲存格。您可以使用透過已簽署萬用字元憑證進行 HTTPS 和主控台 Proxy 通訊的應用裝置部署，為其他儲存格設定已簽署萬用字元 SSL 憑證。

## 必要條件

- 確認在主要應用裝置上提供了包含用於 HTTPS 和主控台 Proxy 別名的已簽署萬用字元 SSL 憑證的金鑰儲存區，即 `/opt/vmware/vcloud-director/certificates.ks`。
  - 如果您需要建立金鑰配對並匯入 CA 簽署的憑證檔案，請參閱[建立 CA 簽署的 SSL 憑證並將其匯入至 vCloud Director 應用裝置](#)。
  - 如果您已有自己的私密金鑰和 CA 簽署的憑證檔案，請參閱[將私密金鑰和 CA 簽署的 SSL 憑證匯入至 vCloud Director 應用裝置](#)。
- 確認金鑰儲存區中金鑰的私人密碼與金鑰儲存區的密碼相符。金鑰儲存區密碼必須符合部署所有應用裝置時使用的初始 root 密碼，例如，

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

。

## 程序

- 1 將包含妥善簽署憑證的新 `certificates.ks` 檔案從主要應用裝置複製到傳輸共用 (位於 `/opt/vmware/vcloud-director/data/transfer/`)。
- 2 將金鑰儲存區檔案的擁有者和群組權限變更為 `vcloud`。

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

- 3 確認金鑰儲存區檔案的擁有者具有讀取和寫入權限。

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

- 4 在主要應用裝置上，執行命令以將新簽署的憑證匯入到 vCloud Director 執行個體中。  
此命令也會更新傳輸共用中的 `responses.properties` 檔案，從而修改 `user.keystore.path` 變數以指向傳輸共用中的金鑰儲存區檔案。

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

- 5 為了使新簽署的憑證生效，請重新啟動主要應用裝置上的 `vmware-vcd` 服務。

```
service vmware-vcd restart
```

- 6 使用與金鑰儲存區密碼相符的初始 root 密碼，部署待命儲存格和應用程式儲存格應用裝置。

## 結果

使用相同 NFS 共用傳輸服務儲存區的所有新部署的應用裝置均已設定主要應用裝置所使用的相同已簽署萬用字元 SSL 憑證。

## 建立 CA 簽署的 SSL 憑證並將其匯入至 vCloud Director 應用裝置

建立與匯入憑證授權機構 (CA) 簽署的憑證為 SSL 通訊提供了最高層級的信任，並有助於保護雲端內的連線安全。

每個 vCloud Director 伺服器都需要兩個 SSL 憑證，才能確保用戶端與伺服器之間安全通訊。每個 vCloud Director 伺服器必須支援兩個不同的 SSL 端點 - 針對 HTTPS 和主控台 Proxy 通訊。

在 vCloud Director 應用裝置中，這兩個端點共用相同的 IP 位址或主機名稱，但使用兩個不同的連接埠 - 將連接埠 443 用於 HTTPS，將 8443 用於主控台 Proxy 通訊。每個端點必須具有其專屬的 SSL 憑證。您可以針對兩個端點使用相同的憑證，例如，使用萬用字元憑證。

兩個端點的憑證皆必須包含 X.500 辨別名稱和 X.509 主體別名延伸。

如果您已有個人私密金鑰和 CA 簽署的憑證檔案，請依照[將私密金鑰和 CA 簽署的 SSL 憑證匯入至 vCloud Director 應用裝置](#)中所述的程序進行操作。

---

**重要** 部署時，vCloud Director 應用裝置會產生金鑰大小為 2048 位元的自我簽署憑證。必須先評估安裝的安全性需求，然後再選擇適當的金鑰大小。根據 NIST 特刊 800-131A，小於 1024 位元的金鑰大小不再受到支援。

---

此程序中使用的金鑰儲存區密碼為 **root** 使用者密碼，其表示為 *root\_passwd*。

### 必要條件

自行熟悉 `keytool` 命令。您可以使用 `keytool` 將 CA 簽署的 SSL 憑證匯入至 vCloud Director 應用裝置。vCloud Director 將 `keytool` 的複本置於 `/opt/vmware/vcloud-director/jre/bin/keytool` 中。

### 程序

- 1 以 **root** 身分直接登入或使用 SSH 登入 vCloud Director 應用裝置主控台。
- 2 視您的環境需求而定，請選擇下列其中一個選項。

當您部署 vCloud Director 應用裝置時，vCloud Director 會自動為 HTTPS 服務和主控台 Proxy 服務產生金鑰大小為 2048 位元的自我簽署憑證。

- 如果想讓憑證授權機構在部署時簽署已產生的憑證，請跳至[步驟 步驟 5](#)。
- 如果您想要使用自訂選項 (例如，較大的金鑰大小) 產生新憑證，請繼續[步驟 步驟 3](#)。

- 3 執行命令以備份現有 `certificates.ks` 檔案。

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

- 4 執行命令，為 HTTPS 服務和主控台 Proxy 服務建立公用和私密金鑰配對。

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

此命令會以您指定的密碼在 `certificates.ks` 中建立或更新金鑰儲存區。已使用命令的預設值建立憑證。視環境的 DNS 組態而定，簽發者一般名稱 (CN) 將設定為每個服務的 IP 位址或 FQDN。此憑證使用預設的 2048 位元金鑰長度，並在建立後一年到期。

**重要** 由於 vCloud Director 應用裝置中的組態限制，您必須使用憑證金鑰儲存區的 `/opt/vmware/vcloud-director/certificates.ks` 位置。

**備註** 您可以使用應用裝置 `root` 密碼做為金鑰儲存區密碼。

## 5 為 HTTPS 服務和主控台 Proxy 服務建立憑證簽署要求 (CSR)。

**重要** vCloud Director 應用裝置會針對 HTTPS 服務和主控台 Proxy 服務共用相同的 IP 位址和主機名稱。因此，CSR 建立命令必須為主體別名 (SAN) 延伸引數提供相同的 DNS 和 IP。

### a 在 `http.csr` 檔案中建立憑證簽署要求。

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

### b 在 `consoleproxy.csr` 檔案中建立憑證簽署要求。

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

## 6 傳送憑證簽署要求到您的憑證授權機構。

如果您的憑證授權單位要求您指定網頁伺服器類型，請使用 Jakarta Tomcat。

取得 CA 簽署憑證。

## 7 將 CA 簽署的憑證、CA 根憑證和任何中繼憑證複製到 vCloud Director 應用裝置。

## 8 執行命令以將已簽署的憑證匯入至 JCEKS 金鑰儲存區。

### a 將憑證授權機構的根憑證從 `root.cer` 檔案匯入到 `certificates.ks` 金鑰儲存區檔案中。

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

### b 如果收到了中繼憑證，請將其從 `intermediate.cer` 檔案匯入到 `certificates.ks` 金鑰儲存區檔案中。

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

- c 匯入 HTTPS 服務憑證。

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

- d 匯入主控台 Proxy 服務憑證。

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

此命令使用新取得的 CA 簽署的憑證版本來覆寫 certificates.ks 檔案。

- 9 若要確認是否已匯入憑證，請執行命令以列出金鑰儲存區檔案的內容。

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

- 10 執行命令，將憑證匯入至 vCloud Director 執行個體。

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

- 11 為了使新簽署的憑證生效，請重新啟動 vCloud Director 應用裝置上的 vmware-vcd 服務。

```
service vmware-vcd restart
```

#### 後續步驟

- 如果是使用萬用字元憑證，請參閱[使用已簽署的萬用字元憑證部署 vCloud Director 應用裝置以進行 HTTPS 和主控台 Proxy 通訊](#)。
- 如果不是使用萬用字元憑證，請在伺服器群組中的所有 vCloud Director 伺服器上重複此程序。
- 如需有關取代內嵌式 PostgreSQL 資料庫和 vCloud Director 應用裝置管理使用者介面之憑證的詳細資訊，請參閱[取代自我簽署的內嵌式 PostgreSQL 和 vCloud Director 應用裝置管理 UI 憑證](#)。

## 將私密金鑰和 CA 簽署的 SSL 憑證匯入至 vCloud Director 應用裝置

如果您有自己的私密金鑰和 CA 簽署的憑證檔案，必須在 vCloud Director 環境中匯入金鑰儲存區之前，建立用於匯入 HTTPS 和主控台 Proxy 服務的憑證和私密金鑰的金鑰儲存區檔案。

#### 必要條件

- 自行熟悉 keytool 命令。您可以使用 keytool 將 CA 簽署的 SSL 憑證匯入至 vCloud Director 應用裝置。vCloud Director 將 keytool 的複本置於 /opt/vmware/vcloud-director/jre/bin/keytool 中。
- 將您的中繼憑證、根 CA 憑證、CA 簽署的 HTTPS 服務和主控台 Proxy 服務的私密金鑰和憑證複製到應用裝置中。

## 程序

- 1 以 **root** 身分直接登入或使用 SSH 登入 vCloud Director 應用裝置主控台。
- 2 如果您有中繼憑證，請執行命令，將根 CA 簽署的憑證與中繼憑證組合在一起，並建立憑證鏈結。

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

- 3 使用 OpenSSL 為 HTTPS 和主控台 Proxy 服務建立具有私密金鑰、憑證鏈結和相應別名的中繼 PKCS12 金鑰儲存區檔案，並為每個金鑰儲存區檔案指定密碼。
  - a 為 HTTPS 服務建立金鑰儲存區檔案。

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

- b 為主控台 Proxy 服務建立金鑰儲存區檔案。

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

- 4 執行命令以備份現有 `certificates.ks` 檔案。

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

- 5 使用 `keytool` 命令將 PKCS12 金鑰儲存區匯入至 JCEKS 金鑰儲存區。

- a 匯入 HTTPS 服務的 PKCS12 金鑰儲存區。

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

- b 匯入主控台 Proxy 服務的 PKCS12 金鑰儲存區。

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

- 6 確認憑證匯入是否成功。

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

- 7 執行命令以將已簽署的憑證匯入至 vCloud Director 執行個體。

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

- 8 為了使 CA 簽署的憑證生效，請重新啟動 vCloud Director 應用裝置上的 `vmware-vcd` 服務。

```
service vmware-vcd restart
```

## 後續步驟

- 如果是使用萬用字元憑證，請參閱[使用已簽署的萬用字元憑證部署 vCloud Director 應用裝置以進行 HTTPS 和主控台 Proxy 通訊](#)。
- 如果不是使用萬用字元憑證，請在伺服器群組中的所有 vCloud Director 應用裝置儲存格上重複此程序。
- 如需有關取代內嵌式 PostgreSQL 資料庫和 vCloud Director 應用裝置管理使用者介面之憑證的詳細資訊，請參閱[取代自我簽署的內嵌式 PostgreSQL 和 vCloud Director 應用裝置管理 UI 憑證](#)。

## 取代自我簽署的內嵌式 PostgreSQL 和 vCloud Director 應用裝置管理 UI 憑證

依預設，內嵌式 PostgreSQL 資料庫和 vCloud Director 應用裝置管理使用者介面共用一組自我簽署的 SSL 憑證。為提高安全性，您可以將預設的自我簽署憑證取代為憑證授權機構 (CA) 簽署的憑證。

當您部署 vCloud Director 應用裝置時，它會產生有效期間為 365 天的自我簽署憑證。vCloud Director 應用裝置使用兩組 SSL 憑證。vCloud Director 服務將一組憑證用於 HTTPS 和主控台 Proxy 通訊。內嵌式 PostgreSQL 資料庫和 vCloud Director 應用裝置管理使用者介面共用另一組 SSL 憑證。

**備註** 取代資料庫和應用裝置管理 UI 憑證的程序不會影響用於 HTTPS 和主控台 Proxy 通訊的憑證。取代其中一個憑證集並不意味著必須取代另一個憑證集。

### 程序

- 1 將位於 `/opt/vmware/appliance/etc/ssl/vcd_ova.csr` 的憑證簽署要求傳送至 CA 以供簽署。
- 2 如果您要取代主要資料庫的憑證，請將所有其他節點置於維護模式，以避免資料遺失的可能性。
- 3 將 `/opt/vmware/appliance/etc/ssl/vcd_ova.crt` 中的現有 PEM 格式憑證取代為在步驟 1 中從 CA 取得的簽署憑證。
- 4 若要取得新憑證，請重新啟動 `vpostgres`、`nginx` 和 `vcd_ova_ui` 服務。

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

```
systemctl restart vpostgres.service
```

- 5 如果您要取代主要資料庫的憑證，請將所有其他節點移出維護模式。

### 結果

下次執行 `appliance-sync` 函數時，新憑證會匯入至其他 vCloud Director 儲存格上的 vCloud Director 信任存放區中。此作業可能最多需要 60 秒。

## 更新 vCloud Director 應用裝置憑證

當您部署 vCloud Director 應用裝置時，它會產生有效期為 365 天的自我簽署憑證。如果在您的環境中存在即將到期或已到期的憑證，您可以產生新的自我簽署憑證。您必須個別更新每個 vCloud Director 儲存格的憑證。

vCloud Director 應用裝置使用兩組 SSL 憑證。vCloud Director 服務將一組憑證用於 HTTPS 和主控台 Proxy 通訊。內嵌式 PostgreSQL 資料庫和 vCloud Director 應用裝置管理使用者介面共用另一組 SSL 憑證。

您可以變更這兩組自我簽署的憑證。或者，如果您將 CA 簽署的憑證用於 vCloud Director 的 HTTPS 和主控台 Proxy 通訊，則只能變更內嵌式 PostgreSQL 資料庫和應用裝置管理使用者介面憑證。CA 簽署的憑證包含知名公共憑證授權機構頒發的完整信任鏈結。

### 必要條件

如果您要更新資料庫高可用性叢集中的主要節點的憑證，請將所有其他節點置於維護模式，以防止資料遺失。請參閱 [〈管理儲存格〉](#)。

### 程序

- 1 以 **root** 身分直接登入或使用 SSH 登入 vCloud Director 應用裝置的作業系統。
- 2 若要停止 vCloud Director 服務，請執行下列命令。

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

- 3 若要產生新的自我簽署憑證，請執行下列命令。

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

此命令會自動針對內嵌式 PostgreSQL 資料庫和應用裝置管理 UI 使用新產生的憑證。PostgreSQL 和 Nginx 伺服器將重新啟動。此命令會產生新的憑證金鑰儲存區 `/opt/vmware/vcloud-director/certificates.ks`，其中包含用於 vCloud Director 之 HTTPS 和主控台 Proxy 通訊的新自我簽署憑證 (在 [步驟 4](#) 中使用)。

- 4 如果您未使用 CA 簽署的憑證，請執行命令，將新產生的自我簽署憑證匯入 vCloud Director 中。

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

- 5 重新啟動 vCloud Director 服務。

```
service vmware-vcd start
```

### 結果

更新的自我簽署憑證會顯示在 vCloud Director 使用者介面中。

下次執行 `appliance-sync` 函數時，新的 PostgreSQL 憑證會匯入至其他 vCloud Director 儲存格上的 vCloud Director 信任存放區中。此作業可能最多需要 60 秒。

## 後續步驟

如有必要，自我簽署憑證可取代為由外部或內部憑證授權機構簽署的憑證。

# vCloud Director 應用裝置組態

# 8

您可以檢視資料庫 HA 叢集中的儲存格狀態、備份和還原內嵌式資料庫，以及重新設定應用裝置設定。

部署 vCloud Director 應用裝置後，您無法變更應用裝置的 `eth0` 和 `eth1` 網路 IP 位址或主機名稱。如果您想讓 vCloud Director 應用裝置具有不同的位址或主機名稱，則必須部署新的應用裝置。

如果您必須對需要關閉資料庫高可用性叢集的應用裝置執行維護以避免發生同步問題，您必須先關閉主要應用裝置，然後再關閉待命應用裝置。

本章節討論下列主題：

- [檢視資料庫高可用性叢集中的儲存格的狀態](#)
- [從高可用性叢集中的主要資料庫故障復原](#)
- [vCloud Director 應用裝置的內嵌式資料庫備份和還原](#)
- [設定 vCloud Director 資料庫的外部存取權](#)
- [啟用或停用對 vCloud Director 應用裝置的 SSH 存取](#)
- [編輯 vCloud Director 應用裝置的 DNS 設定](#)
- [編輯 vCloud Director 應用裝置網路介面的靜態路由](#)
- [vCloud Director 應用裝置中的組態指令碼](#)
- [在 vCloud Director 應用裝置中修改 PostgreSQL 組態](#)

## 檢視資料庫高可用性叢集中的儲存格的狀態

若要檢視應用裝置資料庫高可用性 (HA) 叢集中的主要和待命儲存格的狀態，您可以登入資料庫 HA 叢集中任何儲存格的應用裝置管理使用者介面。

vCloud Director 應用裝置資料庫 HA 叢集包含一個主要儲存格和兩個待命儲存格。請參閱 [應用裝置部署和資料庫高可用性組態](#)。

### 程序

- 1 在網頁瀏覽器中，前往應用裝置管理使用者介面，網址為 `https://vcd_ip_address:5480`。
- 2 以根使用者身分登入。

- 3 若要檢視有關資料庫 HA 叢集中儲存格的詳細資料，請按一下 **vCD 資料庫可用性**。

屬性	描述
名稱	儲存格的 DNS 名稱。
角色	可以是主要或待命。 應用裝置資料庫 HA 叢集包含一個主要儲存格和兩個待命儲存格。
狀態	可以為執行中、無法連線或失敗。 星號 (*) 表示主要儲存格的狀態。
追縱	待命儲存格複寫所用主要儲存格的名称。

#### 後續步驟

如果待命儲存格不處於執行中狀態，則部署新的待命儲存格。

如果主要儲存格不處於執行中狀態，[從高可用性叢集中的主要資料庫故障復原](#)。

## 從高可用性叢集中的主要資料庫故障復原

如果主要儲存格未正確執行，您可以升階其中一個待命儲存格使其變成新的主要儲存格以復原 vCloud Director 資料庫。之後，您必須部署新的待命儲存格。

#### 必要條件

- 主要儲存格處於無法連線狀態或失敗狀態。
- 兩個待命儲存格都處於執行中狀態。

請參閱 [檢視資料庫高可用性叢集中的儲存格的狀態](#)。

#### 程序

- 1 以**根使用者**身分登入執行中待命儲存格的應用裝置管理使用者介面 `https://standby_ip_address:5480`。
- 2 在您想要將其變成新主要儲存格之待命儲存格的**角色**資料行中，按一下**升階**。  
儲存格變成了處於執行中狀態的新主要儲存格。另一個待命儲存格則跟隨新升階的主要儲存格。
- 3 部署新的待命應用裝置。

#### 後續步驟

- 1 從 vCloud Director 伺服器群組和 repmgr 高可用性叢集移除失敗的主要應用裝置。請參閱 [〈刪除雲端儲存格〉](#)和[解除登錄資料庫高可用性叢集中失敗的主要儲存格](#)。
- 2 如有必要，請刪除失敗的主要應用裝置。

## vCloud Director 應用裝置的內嵌式資料庫備份和還原

您可以備份 vCloud Director 應用裝置的內嵌式 PostgreSQL 資料庫，以協助您在出現故障後還原 vCloud Director 環境。

### 備份 vCloud Director 應用裝置的內嵌式資料庫

如果您的環境包含具有內嵌式 PostgreSQL 資料庫的 vCloud Director 應用裝置部署，您可以從主要儲存格備份 vCloud Director 資料庫。產生的 .tgz 檔案會儲存在 NFS 共用傳輸服務儲存區的位置上。

#### 程序

- 1 以 **root** 身分直接登入或使用 SSH 登入主要儲存格。
- 2 導覽至 `/opt/vmware/appliance/bin`。
- 3 執行 `create-db-backup` 命令。

#### 結果

在 NFS 共用傳輸服務儲存區的 `vcloudapp.nfs_mount.VMware_vCloud_Director/pgdb-backup/` 目錄中，您可以看到新建立的 `db-backup-date_time_format.tgz` 檔案。 .tgz 檔案包含資料庫傾印檔案，以及主要儲存格的 `global.properties`、`responses.properties`、`certificates` 和 `proxycertificates` 檔案。

### 還原具有高可用性資料庫組態的 vCloud Director 應用裝置環境

如果您已備份具有 HA 資料庫組態的 vCloud Director 應用裝置環境的內嵌式 PostgreSQL 資料庫，則可以部署新的應用裝置叢集，並在其中還原應用裝置資料庫。

若要還原具有非 HA 資料庫組態的應用裝置部署，請參閱 [還原不具有高可用性資料庫組態的 vCloud Director 應用裝置環境](#)。

還原工作流程包括三個主要階段。

- 從傳輸服務 NFS 共用儲存區複製內嵌式資料庫備份 .tar 檔案。
- 將資料庫還原到內嵌式資料庫的主要儲存格和待命儲存格。
- 部署任何所需的應用程式儲存格。

#### 先決條件

- 確認您具有內嵌式 PostgreSQL 資料庫的備份 .tar 檔案。請參閱 [備份 vCloud Director 應用裝置的內嵌式資料庫](#)。
- 部署一個主要資料庫儲存格和兩個待命資料庫儲存格。請參閱第 6 章 [部署 vCloud Director 應用裝置](#)。
- 如果您想讓新應用裝置叢集使用先前環境的 NFS 伺服器，請建立並匯出此 NFS 伺服器上的新目錄做為新共用項目。無法重複使用現有的掛接點。

## 程序

- 1 在主要和待命儲存格上，以 **root** 身分登入，然後執行命令以停止 vCloud Director 服務。

```
service vmware-vcd stop
```

- 2 在主要和待命儲存格上，將備份 **.tar** 檔案複製到 **/tmp** 資料夾。  
如果 **/tmp** 資料夾上沒有足夠的可用空間，請使用其他位置來儲存 **.tar** 檔案。
- 3 在主要和待命儲存格上，解壓縮位於 **/tmp** 的備份檔案。

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

在 **/tmp** 資料夾中，您可以看到解壓縮的 **global.properties**、**responses.properties**、**certificates**、**proxycertificates**、**truststore**，以及名為 **vcloud\_***date\_time\_format* 的資料庫傾印檔案。

---

**備註** **truststore** 檔案僅適用於 vCloud Director 9.7.0.1 及更新版本。

---

- 4 僅在主要儲存格上，以 **root** 身分登入主控台，然後執行下列命令。
  - a 捨棄 **vcloud** 資料庫。

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

- b 執行 **pg\_restore** 命令。

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

- 5 在主要和待命儲存格上，儲存組態資料檔案的複本，取代這些檔案，然後重新設定並啟動 vCloud Director 服務。
  - a 備份內容、憑證和信任存放區檔案。

**global.properties**、**responses.properties**、**certificates**、**proxycertificates** 和 **truststore** 檔案位於 **/opt/vmware/vcloud-director/etc/**。

---

**備註** **truststore** 檔案僅適用於 vCloud Director 9.7.0.1 及更新版本。

---

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

- b 從您在**步驟 3** 中解壓縮的備份檔案中，複製並取代內容、憑證和信任存放區檔案。

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

**備註** truststore 檔案僅適用於 vCloud Director 9.7.0.1 及更新版本。

```
cp certificates /optvmware/vcloud-director/.
```

- c 備份 /opt/vmware/vcloud-director/certificates.ks 中的金鑰儲存區檔案。

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

- d 執行命令以重新設定 vCloud Director 服務。

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

其中：

- --keystore-password 選項符合應用裝置上憑證的金鑰儲存區密碼。
- --database-password 選項符合您在應用裝置部署期間設定的資料庫密碼。
- --database-host 選項與主要資料庫應用裝置的 eth1 網路 IP 位址相符。
- --primary-ip 值與您要還原的應用裝置儲存格的 eth0 網路 IP 位址相符。這不是主要資料庫儲存格 IP 位址。
- --console-proxy-ip 選項與您要還原的應用裝置的 eth0 網路 IP 位址相符。

如需疑難排解資訊，請參閱[移轉或還原到 vCloud Director 應用裝置時重新設定 vCloud Director 服務失敗](#)。

- e 執行命令以啟動 vCloud Director 服務。

```
service vmware-vcd start
```

您可以在 /opt/vmware/vcloud-director/logs/cell.log 中監控儲存格的啟動進度。

- 6 (選擇性) 部署任何其他應用程式儲存格。請參閱[第 6 章 部署 vCloud Director 應用裝置](#)。

- 7 在伺服器群組的所有儲存格完成啟動程序後，確認 vCloud Director 環境已成功還原。
  - a 使用新伺服器群組中任意儲存格的 eth0 網路 IP 位址 (即 `https://et0_IP_new_cell/cloud`)，開啟 vCloud Director Web Console。
  - b 使用現有的**系統管理員**認證登入 vCloud Director Web Console。
  - c 驗證您的 vSphere 和雲端資源在新環境中是否可用。
- 8 成功驗證資料庫還原之後，使用 vCloud Director Web Console 刪除屬於舊 vCloud Director 環境的已中斷連線的儲存格。
  - a 從**管理與監視**索引標籤，按一下**雲端儲存格**。
  - b 在儲存格名稱上按一下滑鼠右鍵，然後選取**刪除**。

## 還原不具有高可用性資料庫組態的 vCloud Director 應用裝置環境

如果您已備份具有非 HA 資料庫組態的 vCloud Director 應用裝置環境的內嵌式 PostgreSQL 資料庫，則可以部署新的應用裝置叢集，並在其中還原應用裝置資料庫。

若要還原具有 HA 資料庫組態的應用裝置部署，請參閱[還原具有高可用性資料庫組態的 vCloud Director 應用裝置環境](#)。

還原工作流程包括三個主要階段。

- 從傳輸服務 NFS 共用儲存區複製內嵌式資料庫備份 .tar 檔案。
- 將資料庫還原到內嵌式資料庫的主要儲存格。
- 部署任何所需的應用程式儲存格。

### 先決條件

- 確認您具有內嵌式 PostgreSQL 資料庫的備份 .tar 檔案。請參閱[備份 vCloud Director 應用裝置的內嵌式資料庫](#)。
- 部署一個主要資料庫儲存格。請參閱[第 6 章 部署 vCloud Director 應用裝置](#)。
- 如果您想讓新應用裝置叢集使用先前環境的 NFS 伺服器，請建立並匯出此 NFS 伺服器上的新目錄做為新共用項目。無法重複使用現有的掛接點。

### 程序

- 1 在主要儲存格上，以 **root** 身分登入主控台，然後執行命令以停止 vCloud Director 服務。

```
service vmware-vcd stop
```

- 2 將備份 .tar 檔案複製到 /tmp 資料夾。

如果 /tmp 資料夾上沒有足夠的可用空間，請使用其他位置來儲存 .tar 檔案。

- 3 在 /tmp 中解壓縮備份檔案。

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

在 /tmp 資料夾中，您可以看到解壓縮的 `global.properties`、`responses.properties`、`certificates`、`proxycertificates`、`truststore`，以及名為 `vcloud_date_time_format` 的資料庫傾印檔案。

---

**備註** `truststore` 檔案僅適用於 vCloud Director 9.7.0.1 及更新版本。

---

- 4 執行命令以捨棄資料庫，並將其還原至新的應用裝置。

- a 捨棄 vcloud 資料庫。

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

- b 執行 `pg_restore` 命令。

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

- 5 在主要儲存格上，儲存組態資料檔案的複本，取代這些檔案，然後重新設定並啟動 vCloud Director 服務。

- a 備份內容、憑證和信任存放區檔案。

`global.properties`、`responses.properties`、`certificates`、`proxycertificates` 和 `truststore` 檔案位於 `/opt/vmware/vcloud-director/etc/`。

---

**備註** `truststore` 檔案僅適用於 vCloud Director 9.7.0.1 及更新版本。

---

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

- b 從您在步驟 3 中解壓縮的備份檔案中，複製並取代內容、憑證和信任存放區檔案。

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

---

**備註** `truststore` 檔案僅適用於 vCloud Director 9.7.0.1 及更新版本。

---

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

- c 備份 `/opt/vmware/vcloud-director/certificates.ks` 中的金鑰儲存區檔案。

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

- d 執行命令以重新設定 vCloud Director 服務。

```
/opt/vmware/vcloud-director/bin/configure --unattended-installation --database-type postgres --database-user vcloud \
```

```

--database-password db_password_new_primary --database-host eth1_ip_new_primary --database-
port 5432 \
--database-name vcloud --database-ssl true --uuid --keystore /opt/vmware/vcloud-director/
certificates.ks \
--keystore-password ks_password --primary-ip appliance_eth0_ip \
--console-proxy-ip appliance_eth0_ip --console-proxy-port-https 8443

```

其中：

- `--keystore-password` 選項符合應用裝置上憑證的金鑰儲存區密碼。
- `--database-password` 選項符合您在應用裝置部署期間設定的資料庫密碼。
- `--database-host` 選項與主要資料庫應用裝置的 `eth1` 網路 IP 位址相符。
- `--primary-ip` 值與您要還原的應用裝置儲存格的 `eth0` 網路 IP 位址相符。這不是主要資料庫儲存格 IP 位址。
- `--console-proxy-ip` 選項與您要還原的應用裝置的 `eth0` 網路 IP 位址相符。

如需疑難排解資訊，請參閱[移轉或還原到 vCloud Director 應用裝置時重新設定 vCloud Director 服務失敗](#)。

- e 執行命令以啟動 vCloud Director 服務。

```
service vmware-vcd start
```

您可以在 `/opt/vmware/vcloud-director/logs/cell.log` 中監控儲存格的啟動進度。

- 6 (選擇性) 部署任何其他應用程式儲存格。請參閱[第 6 章 部署 vCloud Director 應用裝置](#)。
- 7 在伺服器群組的所有儲存格完成啟動程序後，確認 vCloud Director 環境已成功還原。
  - a 使用新伺服器群組中任意儲存格的 `eth0` 網路 IP 位址 (即 `https://eth0_IP_new_cell/cloud`)，開啟 vCloud Director Web Console。
  - b 使用現有的**系統管理員**認證登入 vCloud Director Web Console。
  - c 驗證您的 vSphere 和雲端資源在新環境中是否可用。
- 8 成功驗證資料庫還原之後，使用 vCloud Director Web Console 刪除屬於舊 vCloud Director 環境的已中斷連線的儲存格。
  - a 從**管理與監視**索引標籤，按一下**雲端儲存格**。
  - b 在儲存格名稱上按一下滑鼠右鍵，然後選取**刪除**。

## 設定 vCloud Director 資料庫的外部存取權

您可以啟用特定外部 IP 位址對內嵌於主要應用裝置的 vCloud Director 資料庫的存取權。

移轉至 vCloud Director 應用裝置期間，或如果您計劃使用第三方資料庫備份解決方案，您可能想要啟用對內嵌式 vCloud Director 資料庫的外部存取權。

**程序**

- 1 以 **root** 身分直接登入或使用 SSH 登入主要儲存格。
- 2 導覽至資料庫目錄 `/opt/vmware/appliance/etc/pg_hba.d/`。
- 3 建立包含目標外部 IP 位址項目的文字檔，類似於：

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

例如：

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

您的項目附加到動態更新的 `pg_hba.conf` 檔案，該檔案控制對 HA 叢集中的主要資料庫的存取權。

## 啟用或停用對 vCloud Director 應用裝置的 SSH 存取

在應用裝置部署期間，您可以保持停用狀態，也可以啟用對應用裝置的 SSH 存取。部署之後，您可以切換 SSH 存取設定。

SSH 精靈會在應用裝置中執行，以用於資料庫 HA 功能及遠端**根**登入。您可以針對**根**使用者停用 SSH 存取。資料庫 HA 功能的 SSH 存取會保持不變。

**程序**

- 1 如果要對 OVF 內容進行暫時變更 (例如，用於測試目的)，請變更 vCloud Director 中的內容。
  - a 以 **root** 身分直接登入或使用 SSH 用戶端登入 vCloud Director 應用裝置主控台。
  - b 執行啟用或停用 SSH **根**存取的指令碼。
    - 若要啟用 SSH **根**存取，請執行 `/opt/vmware/appliance/bin/enable_root_login.sh` 指令碼。
    - 若要停用 SSH **根**存取，請執行 `/opt/vmware/appliance/bin/disable_root_login.sh` 指令碼。
- 2 如果要對 OVF 內容進行永久變更，請使用 vSphere 使用者介面設定 `vcloudapp.enable_ssh.VMware_vCloud_Director` 內容的值。

---

**備註** 您必須關閉虛擬機器的電源，才能在 vSphere 中變更內容的值。

---

- 若要啟用 SSH，請將 `vcloudapp.enable_ssh.VMware_vCloud_Director` 的值設定為 **True**。
- 若要停用 SSH，請將 `vcloudapp.enable_ssh.VMware_vCloud_Director` 的值設定為 **False**。

## 編輯 vCloud Director 應用裝置的 DNS 設定

部署後，您可以變更 vCloud Director 應用裝置的一或多個 DNS 伺服器。

---

**重要** 您無法編輯應用裝置的主機名稱。您必須使用所需的主機名稱部署新的應用裝置。

---

### 程序

- 1 如果要暫時變更 DNS 設定 (例如，用於測試目的)，請在 vCloud Director 中編輯 DNS 設定。
  - a 以 **root** 身分直接登入或使用 SSH 用戶端登入 vCloud Director 應用裝置主控台。
  - b (選擇性) 透過執行下列命令來驗證目前 DNS 組態：

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

- c 變更一或多個 DNS 伺服器。

若要指定多個 DNS 伺服器，請將 *DNS\_server\_IP* 設定為以逗號分隔的清單 (不含空格)。

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

- d 若要使變生效，請重新啟動 VAOS 服務。

```
systemctl restart vaos.service
```

- 2 如果要永久變更 DNS 設定，請使用 vSphere 使用者介面將 *vami.DNS.VMware\_vCloud\_Director* 內容的值設定為新 DNS 伺服器的 IP 位址。

若要指定多個 DNS 伺服器，請輸入以逗號分隔的清單 (不含空格)。

---

**備註** 您必須關閉虛擬機器的電源，才能在 vSphere 中變更內容的值。

---

## 編輯 vCloud Director 應用裝置網路介面的靜態路由

執行初始 vCloud Director 部署後，您可以變更 *eth0* 和 *eth1* 網路介面的靜態路由。

### 程序

- 1 如果要暫時變更靜態路由值 (例如，用於測試目的)，請在 vCloud Director 中編輯靜態路由。
  - a 以 **root** 身分直接登入或使用 SSH 用戶端登入 vCloud Director 應用裝置主控台。
  - b (選擇性) 驗證目前的靜態路由組態。

- 對於 *eth0*，執行下列命令。

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

- 對於 *eth1*，執行下列命令。

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

## c 變更靜態路由值。

靜態路由必須是以逗號分隔的路由規格的清單。例如，對於 eth0，必須執行：

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

- 對於 eth0，執行下列命令。

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

- 對於 eth1，執行下列命令。

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

## d 重新啟動 vCloud Director 應用裝置上的網路服務。

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

## 2 如果要永久變更靜態路由值，請使用 vSphere 使用者介面變更 OVF 內容。

靜態路由必須是以逗號分隔的路由規格的清單。

**備註** 您必須關閉虛擬機器的電源，才能在 vSphere 中變更內容的值。

- 使用 vSphere 使用者介面，將 vcloudnet.routes0.VMware\_vCloud\_Director 內容的值設定為新的路由規格字串。
- 使用 vSphere 使用者介面，將 vcloudnet.routes1.VMware\_vCloud\_Director 內容的值設定為新的路由規格字串。

## vCloud Director 應用裝置中的組態指令碼

vCloud Director 應用裝置包含特定的組態指令碼。

目錄	描述
/opt/vmware/appliance/bin/	應用裝置組態指令碼。
/opt/vmware/appliance/etc/	應用裝置組態檔。
/opt/vmware/appliance/etc/pg_hba.d/	您可以將自訂項目新增至 pg_hba.conf 檔案的目錄。請參閱 <a href="#">設定 vCloud Director 資料庫的外部存取權</a> 。

## 在 vCloud Director 應用裝置中修改 PostgreSQL 組態

您可以使用 PostgreSQL ALTER SYSTEM 命令變更 vCloud Director 應用裝置 PostgreSQL 組態。

ALTER SYSTEM 命令會將參數設定的變更寫入 postgresql.auto.conf 檔案，該檔案在 PostgreSQL 初始化期間優先於 postgresql.conf 檔案。某些設定需要重新啟動 PostgreSQL 服務，而其他設定會以動態方式進行設定，因此不需要重新啟動。請勿變更 postgresql.conf 檔案，因為這些變更在重新開機後不會保留。

**程序**

- 1 以 **root** 身分直接登入或使用 SSH 用戶端登入主要應用裝置的作業系統。
- 2 將使用者變更為 **postgres**。

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

- 3 使用 PostgreSQL ALTER SYSTEM 命令變更參數。

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

- 4 針對每個要變更的組態參數重複 [步驟 3](#)。
- 5 如果您想要變更的某些參數需要重新啟動 PostgreSQL 服務，請重新啟動 vpostgres 程序。

```
systemctl restart vpostgres
```

- 6 如果您的環境中包含待命節點，請將 postgresql.auto.conf 檔案複製到待命應用裝置，並在必要時重新啟動 PostgreSQL 服務。
  - a 將 postgresql.auto.conf 從主要節點複製到待命節點。

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

- b 如果複製的 postgresql.auto.conf 檔案中的某些參數需要重新啟動才能生效，請重新啟動待命節點上的 vpostgres 程序。

```
systemctl restart vpostgres
```

- c 針對每個待命節點重複 [6.a](#) 和 [6.b](#)。

# 在高可用性叢集組態中使用 Replication Manager 工具套件

## 9

repmgr 開放原始碼工具套件是 vCloud Director 應用裝置的內嵌式 PostgreSQL 資料庫的一部分。您可以使用 repmgr 設定、監控和控制 vCloud Director 資料庫高可用性叢集中的 PostgreSQL 複寫和資料庫容錯移轉。

若要檢查節點或叢集的狀態和事件、登錄或解除登錄節點、升階待命節點、交換主要和待命節點的角色，或遵循新的主要節點，您可以使用 repmgr 命令列介面。

若要進一步瞭解 vCloud Director 資料庫高可用性組態，請參閱[應用裝置部署和資料庫高可用性組態](#)。

若要進一步瞭解 repmgr，請造訪 [repmgr.org](http://repmgr.org)。

本章節討論下列主題：

- 檢查資料庫高可用性叢集的連線狀態
- 檢查資料庫高可用性叢集中節點的複寫狀態
- 檢查資料庫高可用性叢集的狀態
- 偵測高可用性叢集中恢復連線的前主要節點
- 在資料庫高可用性叢集中切換主要儲存格和待命儲存格的角色
- 解除登錄資料庫高可用性叢集中失敗或無法連線的待命節點
- 解除登錄資料庫高可用性叢集中失敗的主要儲存格
- 解除登錄資料庫高可用性叢集中正在執行的待命儲存格

## 檢查資料庫高可用性叢集的連線狀態

您可以使用 Replication Manager 工具套件，檢查您的資料庫高可用性叢集中的節點之間的連線。

### 程序

- 1 以 **root** 身分登入或使用 SSH 登入叢集中任何執行中儲存格的作業系統。
- 2 將使用者變更為 **postgres**。

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

### 3 檢查叢集的連線。

- `repmgr cluster matrix` 命令在叢集的每個節點上執行 `repmgr cluster show` 命令，並以矩陣形式顯示結果。

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

在下列範例中，節點 1 和節點 2 已啟動，而節點 3 已關閉。每個資料列對應至一部伺服器，表示該伺服器的輸出連線測試結果。

第三列中的三個項目已標記有嗎？符號，因為節點 3 已關閉，且沒有其輸出連線的相關資訊。

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

- `repmgr cluster crosscheck` 命令交叉檢查每個節點組合之間的連線，可讓您更好地瞭解叢集連線。

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

在下列範例中，執行 `repmgr cluster crosscheck` 命令的節點將其叢集矩陣系統輸出與其他節點輸出進行合併，並且在節點之間執行交叉檢查。在此案例中，所有節點均已啟動，但防火牆會捨棄來自節點 1 並在節點 3 進行導向的封包。這是一個非對稱網路磁碟分割範例，其中，節點 1 無法將封包傳送到節點 3。

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

#### 後續步驟

若要判定資料庫高可用性叢集中的整體連線狀態，請在每個節點上執行這些命令，然後將結果進行比較。

## 檢查資料庫高可用性叢集中節點的複寫狀態

您可以使用 Replication Manager 工具套件和 PostgreSQL 互動式終端機，檢查資料庫高可用性叢集中的個別節點的複寫狀態。

#### 程序

- 1 以 **root** 身分登入或使用 SSH 登入叢集中任何執行中節點的作業系統。

## 2 將使用者變更為 **postgres**。

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

## 3 檢查節點的複寫狀態。

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

系統輸出提供有關節點、PostgreSQL 版本以及複寫詳細資料的資訊。

## 4 (選擇性) 如需更多詳細資訊，請使用 PostgreSQL 互動式終端機檢查節點的複寫狀態。

PostgreSQL 互動式終端機可提供有關待命節點的任何已接收記錄是否落後於主要節點所傳送記錄的資訊。

### a 連線至 **psql** 終端機

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

### b 若要展開顯示並使查詢結果更易於讀取，請執行 **set \x** 命令。

### c 根據節點的角色執行複寫狀態查詢。

選項	動作
在主要節點上執行查詢。	<pre>/opt/vmware/vpostgres/current/bin/psql</pre>
在待命節點上執行查詢。	<pre>select * from pg_stat_wal_receiver;</pre>

## 檢查資料庫高可用性叢集的狀態

若要對資料庫高可用性叢集中的問題進行疑難排解，您必須監控叢集中節點與事件的狀態。

### 程序

#### 1 以 **root** 身分登入或使用 SSH 登入叢集中任何執行中儲存格的作業系統。

#### 2 將使用者變更為 **postgres**。

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

#### 3 檢查叢集的狀態。

**上游**資料行會顯示目前的主要節點。

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

主控台輸出會顯示叢集資訊。在下列範例中，叢集中的主要節點 (節點 3) 的狀態為無法連線。

```

      ID | Name      | Role      | Status      | Upstream      | Location | Connection string
-----+-----+-----+-----+-----+-----+-----
Node 1 | Node name | standby | running     | Node 3 name | default | host=host IP address
user=repmgr dbname=repmgr
Node 2 | Node name | standby | running     | Node 3 name | default | host=host IP address
user=repmgr dbname=repmgr
Node 3 | Node name | primary | ? unreachable |              | default | host=host IP address
user=repmgr dbname=repmgr

```

在下列系統輸出範例中，節點 3 為正常執行的叢集中的主要節點。

```

      ID | Name      | Role      | Status      | Upstream      | Location | Connection string
-----+-----+-----+-----+-----+-----+-----
Node 1 | Node name | standby | running     | Node3 name | default | host=host IP address user=repmgr
dbname=repmgr
Node 2 | Node name | standby | running     | Node3 name | default | host=host IP address user=repmgr
dbname=repmgr
Node 3 | Node name | primary | *running    |              | default | host=host IP address user=repmgr
dbname=repmgr

```

#### 4 檢查叢集事件記錄。

```

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

```

系統輸出會顯示叢集中的建立、複製和登錄事件。

#### 後續步驟

如果主要節點的狀態為無法連線或失敗，則必須升階待命節點。

如果待命節點的狀態為無法連線或失敗，則修復節點並啟動 PostgreSQL 服務 (如果該服務未執行)。

## 偵測高可用性叢集中恢復連線的前主要節點

如果您叢集中的主要節點失敗，然後在將待命節點升階為新的主要節點時恢復連線，則會導致 repmgr 資料不準確。您可以使用 repmgr cluster show 命令偵測異常。

### 範例：在前主要節點上執行 repmgr cluster show

在下列範例中，在恢復連線的前主要節點上執行 repmgr cluster show 命令會產生下列系統輸出。

```

      ID | Name      | Role      | Status      | Upstream      | Location | Connection string
-----+-----+-----+-----+-----+-----+-----
Node 1 | Node1 name | standby | !running as primary | Node 3 name | default | host=host IP address
user=repmgr dbname=repmgr
Node 2 | Node2 name | standby | running     | Node 3 name | default | host=host IP address
user=repmgr dbname=repmgr

```

```
Node 3 | Node3 name | primary | * running | | default | host=host IP address
user=repmgr dbname=repmgr
WARNING: following issues were detected
- node 1(ID: Node 1) is registered as standby but running as primary
```

在此範例中，節點 1 是叢集中的目前主要節點。

執行 `repmgr cluster show` 命令時待命節點顯示 `!running as primary` 狀態，表示前主要節點正在叢集中執行。在此情況下，您必須關閉並解除登錄前主要節點。

## 範例：在新的主要節點上執行 `repmgr cluster show`

在下列範例中，在新的主要節點上執行 `repmgr cluster show` 命令會產生下列系統輸出。

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

在此範例中，`repmgr` 資料是正確的。它準確地指出節點 1 正在執行，並且它是目前的主要節點。關於節點 3 (前主要節點) 的警告訊息指出該節點上的 `repmgr` 資料不準確。

## 範例：升階待命節點後執行 `repmgr cluster show`，但不在剩餘待命節點上執行 `standby follow`

在下列範例中，您可以看到主要節點失敗的叢集中的每個節點上的 `repmgr` 資料。已使用 `repmgr standby promote` 命令手動升階待命節點，但未在剩餘待命節點上執行 `repmgr standby follow`。

當您在主要節點上執行 `repmgr cluster show` 時，系統輸出表示 `repmgr` 資料正確，但新的主要節點 (節點 2) 後面未跟隨任何待命節點。

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

節點 1 (前主要節點) 和節點 3 (跟隨前主要節點的待命節點) 提供的 repmgr 資料不準確。

```

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

```

## 範例：在待命節點上執行 repmgr cluster show

在跟隨目前主要節點的待命節點上執行命令，會產生 repmgr 資料準確的系統輸出，該資料與目前主要節點上的資料相同。

在跟隨前主要節點的待命節點上執行命令，會產生 repmgr 資料不準確的系統輸出，該資料與前主要節點上的資料相同。

## 記錄項目

如果失敗的前主要節點在將待命節點升階為新的主要節點後恢復連線，則會在 repmgr 資料不準確的所有節點上的 update-repmgr-data.log 檔案中顯示下列項目。

```

ERROR: An old primary is running in the repmgr cluster.
ERROR: Manual intervention is required to repair the repmgr cluster.
ERROR: The first step should be to shutdown and unregister the old primary.

```

## 在資料庫高可用性叢集中切換主要儲存格和待命儲存格的角色

在計劃維護期間，您可以使用 repmgr 命令切換資料庫高可用性叢集中的主要節點和其中一個待命節點的角色。

### 必要條件

- 將屬於高可用性叢集的所有 vCloud Director 儲存格置於維護模式。
- 確認叢集中的所有節點皆狀況良好且已上線。

### 程序

- 1 以 **root** 身分登入或使用 SSH 登入您要升階的待命節點的作業系統。
- 2 將使用者變更為 **postgres**。

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

- 3 (選擇性) 執行具有 `--dry-run` 選項的命令，確認是否滿足切換的必要條件。

```
/opt/vmware/vpostgres/current/bin/repmgr standby switchover -f /opt/vmware/vpostgres/current/etc/repmgr.conf --siblings-follow --dry-run
```

- 4 切換主要儲存格和待命儲存格的角色。

```
/opt/vmware/vpostgres/current/bin/repmgr standby switchover -f /opt/vmware/vpostgres/current/etc/repmgr.conf --siblings-follow
```

## 結果

主控台輸出的最後一行指示待命儲存格切換已成功完成。

## 後續步驟

- 1 執行 `reconfigure-database` 命令以更新所有 vCloud Director 儲存格上的資料庫 IP 位址。請參閱 [〈更新 vCloud Director 儲存格上的資料庫 IP 位址〉](#)。
- 2 當您重新設定伺服器群組中的 vCloud Director 儲存格以指向新的主要資料庫時，將屬於高可用性叢集的所有 vCloud Director 儲存格移出維護模式。

## 解除登錄資料庫高可用性叢集中失敗或無法連線的待命節點

您可以在叢集中正在執行的節點上使用 `repmgr`，以解除登錄失敗或無法連線的待命節點。

**備註** 為了使主要節點正常運作，必須至少始終有一個待命節點處於執行狀態。

### 必要條件

若要解除登錄不在執行中的待命節點，您必須提供節點識別碼。若要找到 IP 位址，請檢查叢集的狀態並找到節點。在該資料列中，使用 [連線字串] 資料行中的主機值以識別節點的 IP 位址。請參閱[檢查資料庫高可用性叢集的狀態](#)。

### 程序

- 1 以 `root` 身分登入或使用 SSH 登入叢集的任何執行中節點的作業系統。
- 2 將使用者變更為 `postgres`。

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

- 3 解除登錄失敗或無法連線的節點。

```
/opt/vmware/vpostgres/current/bin/repmgr standby unregister -f /opt/vmware/vpostgres/current/etc/repmgr.conf --node-id=ID
```

## 結果

解除登錄節點會從 `repmgr` 中繼資料移除該節點資訊。

## 解除登錄資料庫高可用性叢集中失敗的主要儲存格

如果您的資料庫高可用性叢集中的主要節點失敗，並且升階了新的主要節點，則必須解除登錄失敗的主要節點，以將其從叢集中移除並避免叢集狀態資料不一致。

### 必要條件

- 若要解除登錄不在執行中的主要節點，您必須提供節點識別碼。若要找到 IP 位址，請檢查叢集的狀態並找到節點。在該資料列中，使用 [連線字串] 資料行中的主機值以識別節點的 IP 位址。請參閱[檢查資料庫高可用性叢集的狀態](#)。
- 確認失敗的主要節點處於非作用中狀態並且未跟隨任何待命節點，然後升階新的主要節點。

### 程序

- 1 以 **root** 身分登入或使用 SSH 登入叢集中任何執行中節點的作業系統。
- 2 將使用者變更為 **postgres**。

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

- 3 (選擇性) 若要確認是否滿足解除登錄節點的必要條件，請執行具有 **--dry-run** 選項的命令。

```
/opt/vmware/vpostgres/current/bin/repmgr primary unregister --node-id=node ID --dry-run
```

- 4 解除登錄節點。

```
/opt/vmware/vpostgres/current/bin/repmgr primary unregister --node-id=node ID
```

### 結果

此作業會從 **repmgr** 中繼資料移除節點。

## 解除登錄資料庫高可用性叢集中正在執行的待命儲存格

如果您想要在其他角色中使用節點，或您想要從高可用性叢集中移除節點，則必須將其解除登錄。

您可以在一般系統作業期間執行此命令。

---

**備註** 為了使主要節點正常運作，必須至少始終有一個待命節點處於執行狀態。

---

### 必要條件

若要解除登錄待命節點，必須提供節點識別碼。若要找到 IP 位址，請檢查叢集的狀態並找到節點。在該資料列中，使用 [連線字串] 資料行中的主機值以識別節點的 IP 位址。請參閱[檢查資料庫高可用性叢集的狀態](#)。

### 程序

- 1 以 **root** 身分登入或使用 SSH 登入叢集中任何執行中節點的作業系統。

## 2 將使用者變更為 **postgres**。

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

## 3 解除登錄節點。

```
/opt/vmware/vpostgres/current/bin/repmgr standby unregister --node-id=node ID -f /opt/vmware/  
vpostgres/current/etc/repmgr.conf
```

### 結果

解除登錄節點會將待命節點的記錄從 **repmgr** 工具套件的內部中繼資料表中移除。

# 安裝 vCloud Director 或部署 vCloud Director 應用裝置之後

# 10

建立 vCloud Director 伺服器群組後，您可以安裝 Microsoft Sysprep 檔案和 Cassandra 資料庫。如果您使用的是 PostgreSQL 資料庫，可以設定 SSL 並調整資料庫上的一些參數。

本章節討論下列主題：

- 在伺服器上安裝 [Microsoft Sysprep 檔案](#)
- [自訂公用端點](#)
- 安裝和設定 [RabbitMQ AMQP Broker](#)
- 安裝並設定 [Cassandra 資料庫](#) 以儲存歷史度量資料
- 在外部 [PostgreSQL 資料庫](#) 上執行其他組態

## 在伺服器上安裝 Microsoft Sysprep 檔案

如果您的雲端需要某些舊版 Microsoft 作業系統的客體自訂支援，則必須在伺服器群組的每個成員上安裝適當的 Microsoft Sysprep 檔案。

只有某些舊版 Microsoft 作業系統需要 Sysprep 檔案。如果在這些作業系統中您的雲端不需要支援客體自訂，則不必安裝 Sysprep 檔案。

若要安裝 Sysprep 二進位檔案，請將這些檔案複製至伺服器上的特定位置。您必須將檔案複製至伺服器群組的每個成員。

### 必要條件

請確認您可以存取 Windows 2003 及 Windows XP 的 32 和 64 位元 Sysprep 二進位檔案。

### 程序

- 1 以**根使用者**身分登入目標伺服器。
- 2 將目錄變更為 `$VCLLOUD_HOME/guestcustomization/default/windows`。

```
[root@cell11 /]# cd /opt/vmware/vcloud-director/guestcustomization/default/windows
```

- 3 建立名稱為 `sysprep` 的目錄。

```
[root@cell11 /opt/vmware/vcloud-director/guestcustomization/default/windows]# mkdir sysprep
```

- 針對需要 Sysprep 二進位檔案的每一個客體作業系統，建立 `$VCLLOUD_HOME/guestcustomization/default/windows/sysprep` 的子目錄。

子目錄名稱是客體作業系統的專屬名稱。

表 10-1. Sysprep 檔案的子目錄指定

客體作業系統	要在 <code>\$VCLLOUD_HOME/guestcustomization/default/windows/sysprep</code> 下方建立的子目錄
Windows 2003 (32 位元)	svr2003
Windows 2003 (64 位元)	svr2003-64
Windows XP (32 位元)	xp
Windows XP (64 位元)	xp-64

例如，若要建立子目錄來儲存適用於 Windows XP 的 Sysprep 二進位檔案，請使用下列 Linux 命令。

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

- 將 Sysprep 二進位檔案複製至伺服器群組中每一部 vCloud Director 伺服器上的適當位置。
- 請確定使用者 `vcloud.vcloud` 可以讀取 Sysprep 檔案。

使用 Linux `chown` 命令執行此作業。

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

## 結果

當 Sysprep 檔案複製至伺服器群組的所有成員時，您可以在雲端中的虛擬機器上執行客體自訂。複製 Sysprep 檔案之後，無須重新啟動 vCloud Director。

## 自訂公用端點

若要滿足負載平衡器或 Proxy 需求，您可以變更 vCloud Director Web 主控台、vCloud API、租用戶入口網站和主控台 Proxy 的預設端點網址。

如果已部署 vCloud Director 應用裝置，您必須設定 vCloud Director 公用主控台 Proxy 位址，因為該應用裝置將具有自訂連接埠 8443 的單一 IP 位址用於主控台 Proxy 服務。請參閱[步驟 5](#)。

### 必要條件

僅系統管理員可以自訂公用端點。

### 程序

- 按一下 **管理索引** 標籤，然後在左窗格中按一下 **公用位址**。
- 選取自訂公用端點。

取消選取此核取方塊會將所有端點還原為其預設值，這些值未在頁面上顯示。

**3** 若要自訂 vCloud REST API 和 OpenAPI URL，請編輯 **API** 端點。

**a** 輸入自訂 HTTP 基底 URL。

例如，如果您將 HTTP 基底 URL 設定為 **http://vcloud.example.com**，您可以存取位於 **http://vcloud.example.com/api** 的 vCloud API，並且可以存取位於 **http://vcloud.example.com/cloudapi** 的 vCloud OpenAPI。

**b** 輸入自訂 HTTPS REST API 基底 URL，然後按一下**瀏覽**來為該端點上傳建立信任鏈結的憑證。

例如，如果您將 HTTPS REST API 基底 URL 設定為 **https://vcloud.example.com**，您可以存取位於 **https://vcloud.example.com/api** 的 vCloud API，並且可以存取位於 **https://vcloud.example.com/cloudapi** 的 vCloud OpenAPI。

憑證鏈結必須符合服務端點使用的憑證，該憑證是上傳到別名為 **http** 之每個 vCloud Director 儲存格金鑰儲存區的憑證或負載平衡器 VIP 憑證 (如果使用 SSL 終止)。憑證鏈結必須包含採用 PEM 格式且不含私密金鑰的端點憑證、中繼憑證和根憑證。

**4** 若要自訂 vCloud Director 租用戶入口網站 URL，請編輯**租用戶入口網站**端點。

- 若要設定 vCloud Director 租用戶入口網站以使用您在**步驟 步驟 3** 中指定的相同端點和憑證鏈結，請選取**複製 API URL 設定**。

- 若要設定 vCloud Director 租用戶入口網站以使用不同的端點和憑證鏈結，請執行下列步驟。

**a** 取消選取**複製 API URL 設定**。

**b** 輸入自訂 HTTP 基底 URL。

例如，如果您將 HTTP 基底 URL 設定為 **http://vcloud.example.com**，您可以存取位於 **http://vcloud.example.com/tenant/org\_name** 的租用戶入口網站。

**c** 輸入自訂 HTTPS REST API 基底 URL，然後按一下**瀏覽**來為該端點上傳建立信任鏈結的憑證。

例如，如果您將 HTTPS REST API 基底 URL 設定為 **https://vcloud.example.com**，您可以存取位於 **https://vcloud.example.com/tenant/org\_name** 的租用戶入口網站。

憑證鏈結必須符合服務端點使用的憑證，該憑證是上傳到別名為 **http** 之每個 vCloud Director 儲存格金鑰儲存區的憑證或負載平衡器 VIP 憑證 (如果使用 SSL 終止)。憑證鏈結必須包含採用 PEM 格式且不含私密金鑰的端點憑證、中繼憑證和根憑證。

5 若要自訂 vCloud Director Web Console URL 和主控台 Proxy 位址，請編輯 **Web 主控台** 端點。

a 針對 HTTP 連線輸入自訂 vCloud Director 公用 URL。

URL 必須包含 /cloud。

例如，如果您將 vCloud Director 公用 URL 設定為 **http://vcloud.example.com/cloud**，您可以存取位於 **http://vcloud.example.com/cloud** 的 vCloud Director Web Console。

b 針對 HTTPS 連線輸入自訂 REST API URL，然後按一下 **瀏覽** 來為該端點上傳建立信任鏈結的憑證。

URL 必須包含 /cloud。

例如，如果您將基底 URL 設定為 **https://vcloud.example.com**，您可以存取位於 **https://vcloud.example.com/cloud** 的 vCloud Director Web Console。

憑證鏈結必須符合服務端點使用的憑證，該憑證是上傳到別名為 **HTTP** 之每個 vCloud Director 儲存格金鑰儲存區的憑證或負載平衡器 VIP 憑證 (如果使用 SSL 終止)。憑證鏈結必須包含採用 PEM 格式且不含私密金鑰的端點憑證、中繼憑證和根憑證。

c 輸入自訂 vCloud Director 公用主控台 Proxy 位址。

此位址是具有連接埠號碼的 vCloud Director 伺服器或負載平衡器的完整網域名稱 (FQDN)。預設連接埠為 443。

---

**重要** vCloud Director 應用裝置將具有自訂連接埠 8443 的 eth0 NIC 用於主控台 Proxy 服務。

---

不支援對負載平衡器中的主控台 Proxy 連線進行 SSL 終止。主控台 Proxy 憑證會上傳到別名為 **consoleproxy** 的每個 vCloud Director 儲存格金鑰儲存區。

例如，對於具有 FQDN **vcloud.example.com** 的 vCloud Director 應用裝置執行個體，輸入 **vcloud.example.com:8443**。

在虛擬機器上開啟遠端主控台視窗時，vCloud Director Web 主控台會使用主控台 Proxy 位址。

6 若要儲存變更，請按一下 **套用**。

## 安裝和設定 RabbitMQ AMQP Broker

AMQP (進階訊息佇列通訊協定) 是訊息佇列的開放標準，可支援企業系統的彈性傳訊。vCloud Director 使用 RabbitMQ AMQP Broker 來提供延伸服務、物件延伸和通知所使用的訊息匯流排。

### 程序

1 從 <https://www.rabbitmq.com/download.html> 下載 RabbitMQ 伺服器。

如需支援的 RabbitMQ 版本清單，請參閱《vCloud Director 版本說明》。

2 遵循 RabbitMQ 安裝指示，在支援的主機上安裝 RabbitMQ。

每一個 vCloud Director 儲存格必須可在網路上到達 RabbitMQ 伺服器主機。

3 安裝 RabbitMQ 期間，請記下您將 vCloud Director 設定為使用此 RabbitMQ 安裝時所需要的值。

- RabbitMQ 伺服器主機的完整網域名稱，例如 *amqp.example.com*。

- 向 RabbitMQ 驗證時有效的使用者名稱及密碼。
- 代理程式接聽訊息的连接埠。預設值為 5672。
- RabbitMQ 虛擬主機。預設值為 "/"。

### 後續步驟

依預設，vCloud Director AMQP 服務會傳送未加密的訊息。您可以設定 AMQP 服務，以使用 SSL 加密這些訊息。此外，還可以設定服務，以使用 vCloud Director 儲存格上 Java Runtime Environment 的預設 JCEKS 信任存放區 (通常位於 `$VCLLOUD_HOME/jre/lib/security/cacerts`) 來驗證代理憑證。

若要對 vCloud Director AMQP 服務啟用 SSL，請執行下列動作：

- 1 在 vCloud Director Web 主控台中，按一下**管理**索引標籤，然後按一下**擴充性**。
- 2 按一下**擴充性**，然後按一下**設定**索引標籤。
- 3 在 **AMQP Broker 設定**區段中，選取**使用 SSL**。
- 4 選取**接受所有憑證**核取方塊，或提供下列其中一個項目：
  - SSL 憑證路徑名稱
  - JCEKS 信任存放區路徑名稱及密碼

## 安裝並設定 Cassandra 資料庫以儲存歷史度量資料

vCloud Director 可以針對您雲端中的虛擬機器，收集可提供虛擬機器效能與資源使用量之最新資訊與歷史資訊的度量。歷史度量資料儲存在 Cassandra 叢集中。

Cassandra 是一個開放原始碼資料庫，您可用於為可擴充的高效能解決方案提供支援存放區，以收集時間序列資料，例如虛擬機器度量。如果您想讓 vCloud Director 支援從虛擬機器擷取歷史度量，則必須安裝並設定 Cassandra 叢集，並且使用 `cell-management-tool` 將叢集連線至 vCloud Director。擷取目前的度量不需要使用選用的資料庫軟體。

### 必要條件

- 請確認 vCloud Director 已安裝並執行，然後再設定選用的資料庫軟體。
- 如果您還未熟悉 Cassandra，請檢閱 <http://cassandra.apache.org/> 上的資料。
- 請參閱《vCloud Director 版本說明》，取得支援用作度量資料庫的 Cassandra 版本清單。您可以從 <http://cassandra.apache.org/download/> 下載 Cassandra。
- 安裝和設定 Cassandra 叢集：
  - Cassandra 叢集必須包括至少四個部署在兩台或更多台主機上的虛擬機器。
  - 需要兩個 Cassandra 種子節點。
  - 啟用 Cassandra 用戶端到節點的加密。請參閱 <http://docs.datastax.com/en/cassandra/3.0/cassandra/configuration/secureSSLIntro.html>。
  - 啟用 Cassandra 使用者驗證。請參閱 <http://docs.datastax.com/en/cassandra/3.0/cassandra/configuration/secureConfigNativeAuth.html>。

- 在每個 Cassandra 叢集上啟用 Java Native Access (JNA) 3.2.7 版或更新版本。
- Cassandra 節點到節點的加密是選擇性的。
- 將 SSL 與 Cassandra 搭配使用是選擇性的。如果您決定不為 Cassandra 啟用 SSL，則必須在每個儲存格上的 `global.properties` 檔案中 (`$VCLLOUD_HOME/etc/global.properties`) 將組態參數 `cassandra.use.ssl` 設定為 0

## 程序

- 1 使用 `cell-management-tool` 公用程式設定 vCloud Director 與 Cassandra 叢集中節點之間的連線。

在下列範例命令中，`node1-ip`、`node2-ip`、`node3-ip` 和 `node4-ip` 是 Cassandra 叢集的成員的 IP 位址。將使用預設連接埠 (9042)。會將度量資料保留 15 天。

```
[root@cell1 /opt/vmware/vcloud-director/
bin]# ./cell-management-tool cassandra --configure --create-schema \ --cluster-nodes node1-
ip,node2-ip,node3-ip, node4-ip \ --username admin --password 'P@55w0rd' --ttl 15
```

如需使用儲存格管理工具的相關資訊，請參閱《vCloud Director 管理員指南》。

- 2 (選擇性) 如果要從版本 9.1 升級 vCloud Director，請使用 `cell-management-tool` 將度量資料庫設定為儲存彙總度量。

執行類似於下列範例的命令：

```
[root@cell1 /opt/vmware/vcloud-director/
bin]# ./cell-management-tool cassandra --add-rollup \ --username admin --password 'P@55w0rd'
```

- 3 重新啟動每個 vCloud Director 儲存格。

## 在外部 PostgreSQL 資料庫上執行其他組態

建立 vCloud Director 伺服器群組後，您可以將外部 PostgreSQL 資料庫設定為需要來自 vCloud Director 儲存格的 SSL 連線，並調整部分資料庫參數以獲得最佳效能。

最安全的連線需要良好簽署的 SSL 憑證，其包含源於已知公開憑證授權機構的完整信任鏈結。或者，您可以使用自我簽署的 SSL 憑證或由私人憑證授權機構簽署的 SSL 憑證，但您必須將該憑證匯入至 vCloud Director 信任存放區。

若要根據您的系統規格和需求取得最佳效能，您可以調整資料庫組態檔中的資料庫組態和 `autovacuum` 參數。

## 程序

### 1 設定 vCloud Director 與 PostgreSQL 資料庫之間的 SSL 連線。

- a 如果針對外部 PostgreSQL 資料庫使用自我簽署的憑證或私人憑證，請從每個 vCloud Director 儲存格執行下列命令，將資料庫憑證匯入 vCloud Director 信任存放區。

```
[root@cell1 /opt/vmware/vcloud-director/bin]#
cell-management-tool import-trusted-certificates --source path_to_self-signed_or_private_cert
```

- b 執行下列命令以啟用 vCloud Director 與 PostgreSQL 之間的 SSL 連線。

```
[root@cell1 /opt/vmware/vcloud-director/bin]#
cell-management-tool reconfigure-database --database-ssl true
```

您可以使用 `--private-key-path` 選項對伺服器群組中的所有儲存格執行下列命令。

```
[root@cell1 /opt/vmware/vcloud-director/bin]#
cell-management-tool reconfigure-database --database-ssl true --private-key-path
path_to_private_key
```

如需有關使用儲存格管理工具的詳細資訊，請參閱《vCloud Director 管理員指南》。

### 2 根據您的系統規格，編輯 `postgresql.conf` 檔案中的資料庫組態。

例如，針對具有 16 GB 記憶體的系统，您可以使用下列片段。

```
max_connections = 500
# Set effective cache size to 50% of total memory.
effective_cache_size = 8GB
# Set shared buffers to 25% of total memory
shared_buffers = 4GB
```

### 3 根據您的需求，編輯 `postgresql.conf` 檔案中的 `autovacuum` 參數。

對於一般 vCloud Director 工作負載，您可以使用下列片段。

```
autovacuum = on
track_counts = on
autovacuum_max_workers = 3
autovacuum_naptime = 1min
autovacuum_vacuum_cost_limit = 2400
```

系統會為活動設定自訂 `autovacuum_vacuum_scale_factor` 值以及 `activity_parameters` 資料表。

## 後續步驟

如果您已編輯 `postgresql.conf` 檔案，必須重新啟動資料庫。

# 升級 vCloud Director 和修補 vCloud Director 應用裝置

# 11

您可以執行有組織的升級、將 vCloud Director 手動升級至新版本，或將修補程式套用至 vCloud Director 應用裝置部署。

如果現有 vCloud Director 伺服器群組包含 Linux 上的 vCloud Director 安裝，您可以使用適用於 Linux 的 vCloud Director 安裝程式來升級您的環境。或者，您可以將環境移轉至 vCloud Director 9.7 應用裝置。請參閱第 12 章 [移轉至 vCloud Director 應用裝置](#)。

如果現有 vCloud Director 伺服器群組包含 vCloud Director 9.5 應用裝置部署，您只能將環境移轉至 vCloud Director 9.7 應用裝置。您可以使用適用於 Linux 的 vCloud Director 安裝程式，以僅在移轉工作流程期間升級現有環境。請參閱第 12 章 [移轉至 vCloud Director 應用裝置](#)。

您可以對 [vCloud Director 安裝](#) 進行有組織地升級或手動升級 [vCloud Director 安裝](#)。透過有組織的升級，執行單一命令即可升級伺服器群組中的所有儲存格和資料庫。透過手動升級，依序升級每個儲存格和資料庫。

從 vCloud Director 9.5 開始：

- Oracle 資料庫不受支援。如果您的現有 vCloud Director 安裝使用 Oracle 資料庫，請參閱[升級使用 Oracle 資料庫的 vCloud Director 安裝的工作流程](#)。
- 不支援啟用和停用 ESXi 主機。開始升級之前，必須啟用所有 ESXi 主機。您可以使用 vSphere Web Client 將 ESXi 主機置於維護模式。
- vCloud Director 使用具有改進 LDAP 支援的 Java。如果您使用的是 LDAPS 伺服器，為避免 LDAP 登入失敗，您必須確認您具備正確建構的憑證。如需相關資訊，請參閱《Java 8 版本變更》，網址為 <https://www.java.com>。

當您升級 vCloud Director 時，新版本必須與現有安裝的以下元件相容：

- 您目前用於 vCloud Director 資料庫的資料庫軟體。  
如果您的現有 vCloud Director 安裝使用 Oracle 資料庫，請參閱[升級使用 Oracle 資料庫的 vCloud Director 安裝的工作流程](#)。
- 您目前使用的 VMware vSphere® 版本。
- 您目前使用的 VMware NSX® 版本。

如需升級路徑以及 vCloud Director 與其他 VMware 產品及第三方資料庫的相容性的相關資訊，請參閱《VMware 產品互通性對照表》，網址為 [http://partnerweb.vmware.com/comp\\_guide/sim/interop\\_matrix.php](http://partnerweb.vmware.com/comp_guide/sim/interop_matrix.php)。如果打算在 vCloud Director 升級過程中升級 vSphere 或 NSX 元件，則必須在 [第 13 章 升級或移轉 vCloud Director](#) 之後進行升級。

至少升級一個 vCloud Director 伺服器後，您可以升級 vCloud Director 資料庫。資料庫會儲存伺服器執行階段狀態的相關資訊，包括其執行的所有 vCloud Director 工作的狀態。若要確定在升級之後沒有任何無效的工作資訊留在資料庫中，您必須在開始升級之前，確認所有伺服器上沒有任何作用中的工作。

此升級也會保留下列構件，該構件不是儲存在 vCloud Director 資料庫中：

- 本機及全域內容檔會複製至新的安裝。
- 用於客體自訂支援的 Microsoft Sysprep 檔案會複製至新的安裝。

升級需要足夠長的 vCloud Director 停機時間，以便升級伺服器群組中的所有伺服器和資料庫。如果您使用負載平衡器，可以進行設定以傳回一則訊息，例如系統進行升級時處於離線狀態。

## 升級使用 Oracle 資料庫的 vCloud Director 安裝的工作流程

升級使用 Oracle 資料庫的 vCloud Director 安裝之前，您必須從 vCloud Director 9.1 版將資料庫移轉至 PostgreSQL。

- 1 如果目前的 vCloud Director 版本低於 9.1，請升級到 9.1 版。

如需將 vCloud Director 升級至 9.1 版的相關資訊，請參閱《vCloud Director 安裝、設定與升級指南》9.1。

- 2 如果 vCloud Director 安裝版本為 9.1，請將 Oracle 資料庫移轉至 PostgreSQL 資料庫。

如需移轉至 PostgreSQL 資料庫的相關資訊，請參閱《vCloud Director 管理員指南》說明文件中的儲存格管理工具參考。

- 3 從版本 9.1 升級 vCloud Director 安裝。您可以對 [vCloud Director 安裝進行有組織地升級](#) 或 [手動升級 vCloud Director 安裝](#)。

## 修補 vCloud Director 應用裝置部署

您可以修補 vCloud Director 應用裝置，以改善其功能或提高其安全性。請參閱 [修補 vCloud Director 應用裝置部署](#)。將修補程式套用到每個 vCloud Director 應用裝置並完成資料庫升級後，您必須在伺服器群組中重新啟動 vCloud Director 服務使其再次上線。

本章節討論下列主題：

- [對 vCloud Director 安裝進行有組織地升級](#)
- [手動升級 vCloud Director 安裝](#)
- [資料庫升級公用程式參考](#)
- [修補 vCloud Director 應用裝置部署](#)

## 對 vCloud Director 安裝進行有組織地升級

您可以透過執行具有 `--private-key-path` 選項的 vCloud Director 安裝程式，來升級伺服器群組中的所有儲存格以及共用資料庫。

您可以使用適用於 Linux 的 vCloud Director 安裝程式，在支援的 Linux 作業系統上升級包含 vCloud Director 安裝的 vCloud Director 伺服器群組。如果 vCloud Director 伺服器群組包含 vCloud Director 9.5 應用裝置部署，則使用適用於 Linux 的 vCloud Director 安裝程式以僅在移轉工作流程期間升級您現有的環境。請參閱第 12 章 [移轉至 vCloud Director 應用裝置](#)。

vCloud Director for Linux 是以數位簽署的可執行檔形式來散佈，名稱採用 `vmware-vcloud-director-distribution-v` 形式。`v.v-nnnnnn.bin` 格式，其中 `v.v` 代表產品版本，`nnnnnn` 代表組建編號。例如：`vmware-vcloud-director-distribution-8.10.0-3698331.bin`。執行此可執行檔可安裝或升級 vCloud Director。

執行具有 `--private-key-path` 選項的 vCloud Director 安裝程式時，您可以新增 `upgrade` 公用程式的其他命令選項，例如 `--maintenance-cell`。如需資料庫 `upgrade` 公用程式選項的相關資訊，請參閱 [資料庫升級公用程式參考](#)。

### 必要條件

- 確認 vCloud Director 資料庫、vSphere 元件和 NSX 元件與新版本的 vCloud Director 相容。

**重要** 如果您的現有 vCloud Director 安裝使用 Oracle 資料庫，請確認已從 vCloud Director 9.1 版移轉至 PostgreSQL 資料庫。請參閱 [升級使用 Oracle 資料庫的 vCloud Director 安裝的工作流程](#)。

- 驗證您是否具有目標伺服器的 Superuser 認證。
- 如果想要安裝程式驗證安裝檔案的數位簽章，請在目標伺服器上下載並安裝 VMware 公開金鑰。如果已驗證安裝檔案的數位簽章，則在安裝期間不需要再次驗證它。請參閱 [下載並安裝 VMware 公用金鑰](#)。
- 請確認您具備有效的授權金鑰，可使用您要升級的 vCloud Director 軟體版本。
- 確認所有儲存格皆允許 Superuser 在沒有密碼的情況下進行 SSH 連線。若要執行驗證，您可以執行下列 Linux 命令：

```
sudo -u vcloud ssh -i private-key-path root@cell-ip
```

此範例設定您的 `vcloud` 身分識別，然後以根使用者身分在執行 `cell-ip` 時使用 SSH 連線至儲存格，但不提供根使用者密碼。如果本機儲存格上 `private-key-path` 中的私密金鑰可由使用者 `vcloud.vcloud` 讀取，且對應的公開金鑰已在執行 `cell-ip` 時存在於根使用者的 `authorized-keys` 檔案，則命令成功。

**備註** `vcloud` 使用者、`vcloud` 群組和 `vcloud.vcloud` 帳戶是由 vCloud Director 安裝程式建立的，用作 vCloud Director 程序執行時所用的身分識別。`vcloud` 使用者無密碼。

- 確認您的所有 ESXi 主機均已啟用。從 vCloud Director 9.5 開始，不支援已停用的 ESXi 主機。
- 確認伺服器群組中的所有伺服器都可以存取共用的傳輸伺服器儲存區。請參閱 [準備傳輸伺服器儲存區](#)。

- 如果 vCloud Director 安裝使用 LDAPS 伺服器以避免升級後出現 LDAP 登入失敗，請確認您擁有建構正確的 Java 8 Update 181 憑證。如需相關資訊，請參閱《Java 8 版本變更》，網址為 <https://www.java.com>。

## 程序

- 1 以**根使用者**身分登入目標伺服器。

- 2 將安裝檔案下載至目標伺服器。

如果已購買媒體上的軟體，請將安裝檔案複製到目標伺服器可以存取的位置。

- 3 驗證下載的總和檢查碼是否符合下載頁面上公佈的總和檢查碼。

MD5 及 SHA1 總和檢查碼的值會公佈在下載頁面上。請使用適當的工具，驗證已下載的安裝檔案的總和檢查碼是否符合下載頁面上顯示的總和檢查碼。下列格式的 Linux 命令會顯示 *installation-file* 的總和檢查碼。

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

此命令會傳回必須符合下載頁面上的 MD5 總和檢查碼的安裝檔案總和檢查碼。

- 4 確定安裝檔案可以執行。

安裝檔案需要執行權限。若要確定它具有此權限，請開啟主控台、Shell 或終端機視窗，並執行下列 Linux 命令，其中 *installation-file* 是 vCloud Director 安裝檔案的完整路徑名稱。

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

- 5 在主控台、Shell 或終端機視窗中，使用 `--private-key-path` 選項和目標儲存格之私密金鑰的路徑名稱執行安裝檔案。

您可以新增資料庫 `upgrade` 公用程式的其他命令選項。

```
./installation-file --private-key-path /vcloud/.ssh/id_rsa
```

**備註** 無法從路徑名稱內含任何空格字元的目錄執行安裝檔案。

安裝程式偵測到舊版 vCloud Director，並提示您確認升級。

如果安裝程式偵測到 vCloud Director 版本等於或晚於安裝檔案中的版本，則它會顯示錯誤訊息並結束。

- 6 輸入 **y** 並按 Enter 鍵，確認升級。

## 結果

安裝程式將起始下列多儲存格升級工作流程。

- 1 確認目前儲存格主機符合所有需求。
- 2 解壓縮 vCloud Director RPM 套件。
- 3 升級目前儲存格上的 vCloud Director 軟體。

- 4 升級 vCloud Director 資料庫。
- 5 升級剩餘的每個儲存格上的 vCloud Director 軟體，然後重新啟動儲存格上的 vCloud Director 服務。
- 6 重新啟動目前儲存格上的 vCloud Director 服務。

#### 後續步驟

啟動伺服器群組中的所有儲存格上的 vCloud Director 服務。

您現在可以升級與已連接 vCenter Server 系統相關聯的每個 NSX Manager，然後升級 vCenter Server 系統、ESXi 主機和 NSX Edge。

## 手動升級 vCloud Director 安裝

您可以透過執行不帶命令選項的 vCloud Director 安裝程式來升級單一儲存格。重新啟動已升級的儲存格之前，您必須先升級資料庫架構。升級伺服器群組中至少一個儲存格之後，再升級資料庫架構。

您可以使用適用於 Linux 的 vCloud Director 安裝程式，在支援的 Linux 作業系統上升級包含 vCloud Director 安裝的 vCloud Director 伺服器群組。如果 vCloud Director 伺服器群組包含 vCloud Director 9.5 應用裝置部署，則使用適用於 Linux 的 vCloud Director 安裝程式以僅在移轉工作流程期間升級您現有的環境。請參閱第 12 章 [移轉至 vCloud Director 應用裝置](#)。

對於多儲存格 vCloud Director 安裝，您可以對 [vCloud Director 安裝進行有組織地升級](#)，而不是依序手動升級每個儲存格和資料庫。

#### 必要條件

- 確認 vCloud Director 資料庫、vSphere 元件和 NSX 元件與新版本的 vCloud Director 相容。

---

**重要** 如果您的現有 vCloud Director 安裝使用 Oracle 資料庫，請確認已從 vCloud Director 9.1 版移轉至 PostgreSQL 資料庫。請參閱[升級使用 Oracle 資料庫的 vCloud Director 安裝的工作流程](#)。

---

- 確認您擁有 vCloud Director 伺服器群組中伺服器的 Superuser 認證。
- 如果想要安裝程式驗證安裝檔案的數位簽章，請在目標伺服器上下載並安裝 VMware 公開金鑰。如果已驗證安裝檔案的數位簽章，則在安裝期間不需要再次驗證它。請參閱[下載並安裝 VMware 公用金鑰](#)。
- 請確認您具備有效的授權金鑰，可使用您要升級的 vCloud Director 軟體版本。
- 確認您的所有 ESXi 主機均已啟用。從 vCloud Director 9.5 開始，不支援已停用的 ESXi 主機。

#### 程序

##### 1 升級 vCloud Director 儲存格

vCloud Director 安裝程式會驗證目標伺服器是否符合所有升級先決條件，並升級伺服器上的 vCloud Director 軟體。

## 2 升級 vCloud Director 資料庫

從已升級的 vCloud Director 伺服器執行 vCloud Director 資料庫升級工具。在升級共用資料庫之前，不得重新啟動已升級的任何 vCloud Director 伺服器。

### 後續步驟

升級伺服器群組中的所有 vCloud Director 伺服器和資料庫後，您可以啟動所有儲存格上的 vCloud Director 服務。

您可以升級與已連接 vCenter Server 系統相關聯的每個 NSX Manager，之後便可升級 vCenter Server 系統、ESXi 主機和 NSX Edge。

## 升級 vCloud Director 儲存格

vCloud Director 安裝程式會驗證目標伺服器是否符合所有升級先決條件，並升級伺服器上的 vCloud Director 軟體。

vCloud Director for Linux 是以數位簽署的可執行檔形式來散佈，名稱採用 `vmware-vcloud-director-distribution-v` 形式。v.v-nnnnnn.bin 格式，其中 v.v.v 代表產品版本，nnnnnn 代表組建編號。例如：`vmware-vcloud-director-distribution-8.10.0-3698331.bin`。執行此可執行檔可安裝或升級 vCloud Director。

對於多儲存格 vCloud Director 安裝，您必須在 vCloud Director 伺服器群組的每個成員上執行 vCloud Director 安裝程式。

### 程序

1 以根使用者身分登入目標伺服器。

2 將安裝檔案下載至目標伺服器。

如果已購買媒體上的軟體，請將安裝檔案複製到目標伺服器可以存取的位置。

3 驗證下載的總和檢查碼是否符合下載頁面上公佈的總和檢查碼。

MD5 及 SHA1 總和檢查碼的值會公佈在下載頁面上。請使用適當的工具，驗證已下載的安裝檔案的總和檢查碼是否符合下載頁面上顯示的總和檢查碼。下列格式的 Linux 命令會顯示 *installation-file* 的總和檢查碼。

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

此命令會傳回必須符合下載頁面上的 MD5 總和檢查碼的安裝檔案總和檢查碼。

4 確定安裝檔案可以執行。

安裝檔案需要執行權限。若要確定它具有此權限，請開啟主控台、Shell 或終端機視窗，並執行下列 Linux 命令，其中 *installation-file* 是 vCloud Director 安裝檔案的完整路徑名稱。

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

## 5 執行安裝檔案。

若要執行安裝檔案，請輸入其完整路徑名稱，例如：

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

此檔案包括安裝指令碼及內嵌式 RPM 套件。

**備註** 無法從路徑名稱內含任何空格字元的目錄執行安裝檔案。

如果安裝程式偵測到 vCloud Director 版本等於或晚於安裝檔案中的版本，則它會顯示錯誤訊息並結束。

如果安裝程式偵測到舊版 vCloud Director，則系統會提示您確認升級。

## 6 輸入 **y** 並按 Enter 鍵，確認升級。

安裝程式將起始下列升級工作流程。

- a 確認主機符合所有需求。
- b 解壓縮 vCloud Director RPM 套件。
- c 儲存格上所有作用中 vCloud Director 工作完成後，會停止伺服器上的 vCloud Director 服務，並升級已安裝的 vCloud Director 軟體。

如果您未在目標伺服器上安裝 VMware 公開金鑰，安裝程式會顯示下列格式的警告：

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

變更目標伺服器上的現有 `global.properties` 檔案時，安裝程式會顯示下列格式的警告：

```
warning: /opt/vmware/vcloud-director/etc/global.properties created as /opt/vmware/vcloud-director/etc/global.properties.rpmnew
```

**備註** 如果您先前已更新現有 `global.properties` 檔案，則可以從 `global.properties.rpmnew` 擷取這些變更。

## 7 (選擇性) 更新記錄內容。

升級後，新的記錄內容會寫入至檔案 `/opt/vmware/vcloud-director/etc/log4j.properties.rpmnew`。

選項	動作
如果您未變更現有的記錄內容	將此檔案複製至 <code>/opt/vmware/vcloud-director/etc/log4j.properties</code> 。
如果您已變更記錄內容	若要保留所做的變更，請將 <code>/opt/vmware/vcloud-director/etc/log4j.properties.rpmnew</code> 與現有 <code>/opt/vmware/vcloud-director/etc/log4j.properties</code> 檔案進行合併。

## 結果

vCloud Director 升級完成後，安裝程式會顯示一則訊息，其中包含有關舊組態檔位置的資訊。然後，安裝程式會提示您執行資料庫升級工具。

## 後續步驟

如果尚未升級，您可以升級 vCloud Director 資料庫。

對伺服器群組中的每個 vCloud Director 儲存格重複此程序。

---

**重要** 升級伺服器群組中的所有儲存格和資料庫前，請勿啟動 vCloud Director 服務。

---

## 升級 vCloud Director 資料庫

從已升級的 vCloud Director 伺服器執行 vCloud Director 資料庫升級工具。在升級共用資料庫之前，不得重新啟動已升級的任何 vCloud Director 伺服器。

所有執行中及目前已完成的工作相關的詳細資訊都會儲存在 vCloud Director 資料庫中。由於資料庫升級會使此工作資訊失效，因此資料庫升級公用程式會確認升級程序開始時沒有任何工作正在執行。

vCloud Director 伺服器群組中的所有儲存格共用相同的資料庫。無論您要升級多少個儲存格，只需要升級資料庫一次。升級資料庫之後，未升級的 vCloud Director 儲存格將無法連線至資料庫。您必須升級所有儲存格，它們才能連線至已升級的資料庫。

## 必要條件

- 備份現有資料庫。使用您的資料庫軟體廠商建議的程序。
- 確認伺服器群組中的所有 vCloud Director 儲存格處於停止狀態。在升級期間，將停止已升級的儲存格。如果存在尚未升級的 vCloud Director 伺服器，您可以使用儲存格管理工具靜止並關閉其服務。如需有關如何使用儲存格管理工具來管理儲存格的資訊，請參閱《vCloud Director 管理員指南》。
- 如果安裝 vCloud Director 時使用 Oracle 資料庫，則會移轉至 PostgreSQL 資料庫。如需有關移轉至 PostgreSQL 資料庫的資訊，請參閱《vCloud Director 管理員指南》中的儲存格管理工具參考。
- 檢閱[資料庫升級公用程式參考](#)。選項和引數非強制。

## 程序

- 1 執行具有或沒有選項的資料庫 upgrade 公用程式。

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

如果資料庫升級公用程式偵測到 NSX Manager 版本不相容，它會顯示一則警告訊息並取消升級。

- 2 在提示時，輸入 **y** 並按 Enter 鍵確認資料庫升級。
- 3 在提示時，輸入 **y** 並按 Enter 鍵確認已備份資料庫。

如果使用了 `--backup-completed` 選項，公用程式會略過此提示。

- 4 如果公用程式偵測到作用中儲存格，請在提示繼續時輸入 **n** 結束 Shell，然後確認沒有任何儲存格正在執行，並且再試一次透過**步驟 步驟 1**升級。

### 結果

資料庫升級工具會執行並顯示進度訊息。升級完成後，系統會提示您在目前的伺服器上啟動 vCloud Director 服務。

### 後續步驟

輸入 **y** 並按 Enter 鍵，或稍後執行 `service vmware-vcd start` 命令啟動該服務。

您可以啟動已升級的 vCloud Director 伺服器的服務。

您可以升級伺服器群組的其餘 vCloud Director 成員並啟動其服務。請參閱**升級 vCloud Director 儲存格**。

## 資料庫升級公用程式參考

執行 `upgrade` 公用程式時，您可以在命令列中提供設定資訊作為選項和引數。

表 11-1. 資料庫升級公用程式選項和引數

選項	引數	說明
<code>--backup-completed</code>	無	指定您已完成 vCloud Director 的備份。包含此選項時，升級公用程式不會提示您備份資料庫。
<code>--ceip-user</code>	CEIP 服務帳戶的使用者名稱。	如果系統組織中已存在具有此使用者名稱的使用者，升級將失敗。預設值： <code>phone-home-system-account</code> 。
<code>--enable-ceip</code>	選擇下列其中一項： <ul style="list-style-type: none"> <li>■ <code>true</code></li> <li>■ <code>false</code></li> </ul>	指定此安裝是否參與 VMware 客戶經驗改進計劃 (CEIP)。如果在目前組態中未提供且未設為 <code>false</code> ，則預設為 <code>true</code> 。VMware 的客戶經驗改進計劃 (「CEIP」) 提供關於透過 CEIP 收集的資料以及 VMware 使用這些資料之用途的其他資訊，該資訊明載於信任與保證中心，網址為： <a href="http://www.vmware.com/trustvmware/ceip.html">http://www.vmware.com/trustvmware/ceip.html</a> 。您可以使用儲存格管理工具隨時加入或退出此產品的 VMware CEIP。請參閱《vCloud Director 管理員指南》中的〈儲存格管理工具參考〉。

表 11-1. 資料庫升級公用程式選項和引數 (續)

選項	引數	說明
<code>--installer-path</code>	vCloud Director 安裝檔案的完整路徑名稱。使用者 <code>vcloud.vcloud</code> 必須能夠讀取安裝檔案以及用於儲存此安裝檔案的目錄。	此產品參與 VMware 客戶經驗改進計劃 (「CEIP」)。關於透過 CEIP 收集的資料以及 VMware 使用這些資料之用途的詳細資料載於信任與保證中心，網址為 <a href="http://www.vmware.com/trustvmware/ceip.html">http://www.vmware.com/trustvmware/ceip.html</a> 。您可以使用儲存格管理工具隨時加入或退出此產品的 VMware CEIP。請參閱《vCloud Director 管理員指南》中的〈儲存格管理工具參考〉。 需要 <code>--private-key-path</code> 選項。
<code>--maintenance-cell</code>	IP 位址	升級期間以維護模式執行之升級公用程式的儲存格的 IP 位址。此儲存格會在其他儲存格關閉前進入維護模式，並在其他儲存格升級時保持維護模式。其他儲存格已升級且至少其中一個儲存格已重新啟動後，此儲存格會關閉並升級。 需要 <code>--private-key-path</code> 選項。
<code>--multisite-user</code>	多站台系統帳戶的使用者名稱。	vCloud Director 多站台功能會使用此帳戶。如果系統組織中已存在具有此使用者名稱的使用者，升級將失敗。預設值： <code>multisite-system-account</code> 。
<code>--private-key-path</code>	pathname	儲存格之私密金鑰的完整檔案路徑。使用此選項時，伺服器群組中的所有儲存格將在資料庫升級後正常關閉、升級和重新啟動。如需有關此升級工作流程的詳細資訊，請參閱對 <a href="#">vCloud Director 安裝進行有組織地升級</a> 。
<code>--unattended-upgrade</code>	無	指定自動升級

如果您使用 `--private-key-path` 選項，所有儲存格必須設定為允許 Superuser 在沒有密碼的情況下進行 ssh 連線。您可使用類似如下所示的 Linux 命令列來驗證此設定。此範例設定您的 `vcloud` 身分識別，然後以 `root` 身分在執行 `cell-ip` 時使用 ssh 連線至儲存格，但不提供根使用者密碼。

```
sudo -u vcloud ssh -i private-key-path root@cell-ip
```

如果本機儲存格上 `private-key-path` 中的私密金鑰可由使用者 `vcloud.vcloud` 讀取，且相應的公開金鑰已在執行 `cell-ip` 時新增到根使用者的 `authorized-keys` 檔案，則命令成功。

**備註** `vcloud` 使用者、`vcloud` 群組和 `vcloud.vcloud` 帳戶是由 vCloud Director 安裝程式建立的，用作 vCloud Director 程序執行時所用的身分識別。`vcloud` 使用者無密碼。

## 修補 vCloud Director 應用裝置部署

您可以使用可能與產品功能和安全性改進相關的修補程式來更新 vCloud Director 應用裝置。

在修補 vCloud Director 應用裝置部署期間，vCloud Director 服務將停止運作，並且可能會停機一段時間。停機時間取決於修補每個 vCloud Director 應用裝置以及執行 vCloud Director 資料庫升級指令碼所需的時間。vCloud Director 伺服器群組中的工作儲存格數目會減少，直到停止最後一個 vCloud Director 應用裝置上的 vCloud Director 服務。在 vCloud Director HTTP 端點前面正確設定的負載平衡器會停止將流量路由到已停止的儲存格。

將修補程式套用到每個 vCloud Director 應用裝置並完成資料庫升級後，您必須在伺服器群組中重新啟動 vCloud Director 服務使其再次上線。

## 程序

- 1 在網頁瀏覽器中，登入 vCloud Director 應用裝置執行個體的應用裝置管理使用者介面，以識別主要應用裝置 `https://appliance_ip_address:5480`。

記下主要應用裝置名稱。升級資料庫時，您必須使用主要應用裝置名稱。

- 2 將更新套件下載至應用裝置。

vCloud Director 做為可執行檔散佈，其名稱格式為 `VMware_vCloud_Director_v.v.v-  
nnnnnnnn_update.tar.gz`，其中 `v.v.v.v` 代表產品版本，`nnnnnnnn` 代表組建編號。例如，`VMware_vCloud_Director_9.7.0.4248-13560441_update.tar.gz`。

- 3 建立要從中擷取更新套件的 `local-update-package` 目錄。

```
mkdir /tmp/local-update-package
```

- 4 在新建立的目錄中擷取更新套件。

```
tar -zxf VMware_vCloud_Director_v.v.v-  
nnnnnnnn_update.tar.gz \  
-C /tmp/local-update-package
```

- 5 將 `local-update-package` 目錄設為更新存放庫。

```
vamicli update --repo file:///tmp/local-update-package
```

- 6 檢查更新以確認是否建立了正確的存放庫。

```
vamicli update --check
```

修補程式發行版本顯示為可用更新。

- 7 透過執行下列命令來關閉 vCloud Director：

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

- 8 從主要應用裝置，備份 vCloud Director 應用裝置的內嵌式資料庫。

**備註** 如果您要從 vCloud Director 9.7.0.1 升級至更新版本，請手動備份位於 `/opt/vmware/vcloud-director/etc/truststore` 的信任存放區檔案。

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

- 9 套用可用的修補程式。

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

- 10 在每個應用裝置上重複步驟 [步驟 2](#) 至 [步驟 7](#) 以及步驟 [步驟 9](#)。

- 11 從任何應用裝置，執行 vCloud Director 資料庫升級指令碼。

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

- 12 在每個應用裝置上啟動 vCloud Director 服務。

```
service vmware-vcd start
```

# 移轉至 vCloud Director 應用裝置

# 12

從 9.7 版開始，vCloud Director 應用裝置包含具有高可用性功能的內嵌式 PostgreSQL 資料庫。您可以將更早版本的現有 vCloud Director 環境移轉至包含 vCloud Director 9.7 應用裝置部署的 vCloud Director 環境。

您可以移轉包含 Linux 上的 vCloud Director 安裝或 vCloud Director 應用裝置部署的 vCloud Director 環境。您可以移轉使用外部 Microsoft SQL 資料庫或外部 PostgreSQL 資料庫的 vCloud Director 環境。

如果 vCloud Director 環境使用外部 Oracle 資料庫，您必須先在 vCloud Director 9.1 版中將資料庫移轉至 PostgreSQL，然後再移轉至 vCloud Director 應用裝置。如需使用 Oracle 資料庫的 vCloud Director 安裝升級工作流程的相關資訊，請參閱第 11 章 [升級 vCloud Director](#) 和 [修補 vCloud Director 應用裝置](#)。

本章節討論下列主題：

- 將使用外部 Microsoft SQL 資料庫的 vCloud Director 移轉到 vCloud Director 應用裝置
- 將使用外部 PostgreSQL 資料庫的 vCloud Director 移轉到 vCloud Director 應用裝置

## 將使用外部 Microsoft SQL 資料庫的 vCloud Director 移轉到 vCloud Director 應用裝置

如果更早版本的目前 vCloud Director 環境使用外部 Microsoft SQL 資料庫，您可以移轉到包含 vCloud Director 9.7 應用裝置部署的新 vCloud Director 環境。您目前的 vCloud Director 環境可以包含 Linux 上的 vCloud Director 安裝或 vCloud Director 應用裝置部署。新的 vCloud Director 環境可以在高可用性模式下使用應用裝置的內嵌式 PostgreSQL 資料庫。

移轉工作流程包括四個主要階段。

- 透過部署 vCloud Director 9.7 應用裝置的一或多個執行個體，建立新的 vCloud Director 伺服器群組
- 升級現有 vCloud Director 環境
- 將外部資料庫移轉至內嵌式資料庫
- 複製共用傳輸服務資料和憑證資料。

### 程序

- 1 將目前的 vCloud Director 環境升級到 9.7 版，然後升級來源資料庫架構。  
請參閱第 11 章 [升級 vCloud Director](#) 和 [修補 vCloud Director 應用裝置](#)。

- 2 確認移轉來源 vCloud Director 重新啟動成功。
- 3 如果您想讓新 vCloud Director 環境使用現有環境的 IP 位址，請將現有儲存格的 IP 位址變更為臨時 IP 位址。
- 4 如果您想讓新 vCloud Director 環境使用現有環境的 NFS 伺服器，請建立並匯出此 NFS 伺服器上的新目錄做為新的共用 NFS 掛接點。

您無法重複使用現有的掛接點，因為舊 NFS 中使用者的使用者識別碼和群組識別碼 (UID/GID) 可能與新 NFS 中的使用者識別碼和群組識別碼不相符。

- 5 透過部署 vCloud Director 9.7 應用裝置的一或多個執行個體，建立新的伺服器群組。
  - 如果您想要使用資料庫高可用性功能，則部署一個主要儲存格和兩個待命儲存格，並選擇性地部署一或多個 vCD 應用程式儲存格。
  - 如果現有儲存格的 IP 位址已變更為臨時 IP 位址，您可以針對新儲存格使用原始 IP 位址。
  - 如果已匯出現有 NFS 伺服器上的新路徑，您可以針對新環境使用這個新的共用掛接點。

請參閱第 6 章 [部署 vCloud Director 應用裝置](#)。

- 6 在每個現有的儲存格上和每個新部署的儲存格上，執行命令以停止 vCloud Director 服務。

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

- 7 選擇其中一個現有的儲存格來用作移轉來源。  
移轉來源必須有權存取新部署的主要儲存格的 eth1 網路 IP 位址。

- 8 在新的主要儲存格上，允許從移轉來源存取內嵌式資料庫。  
請參閱[設定 vCloud Director 資料庫的外部存取權](#)。

- 9 在移轉來源上執行儲存格管理工具，將外部資料庫移轉至新的主要儲存格中內嵌的資料庫。  
內嵌式資料庫使用應用裝置的 eth1 網路 IP 位址。

```
/opt/vmware/vcloud-director/bin/cell-management-tool dbmigrate -dbhost eth1_IP_new_primary \  
-dbport 5432 -dbuser vcloud -dbname vcloud -dbpassword database_password_new_primary
```

如需使用儲存格管理工具的相關資訊，請參閱《vCloud Director 管理員指南》。

- 10 在每個新部署的儲存格上，備份和取代組態資料，然後重新設定並啟動 vCloud Director 服務。
  - a 備份內容和憑證檔案，然後複製並取代移轉來源中的這些檔案。

`global.properties`、`responses.properties`、`certificates` 和 `proxycertificates` 檔案位於 `/opt/vmware/vcloud-director/etc/`。

**重要** 如果您要移轉至 vCloud Director 版本 9.7.0.1 或更新版本，還必須備份、複製和取代移轉來源中的 `truststore` 檔案以及其他檔案。

- b 備份 `/opt/vmware/vcloud-director/certificates.ks` 中的金鑰儲存區檔案。

請勿從移轉來源複製和取代為金鑰儲存區檔案。

- c 執行命令以重新設定 vCloud Director 服務。

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

其中：

- --keystore-password 值符合此應用裝置的初始 **root** 密碼。
- --database-password 值符合您在應用裝置部署期間設定的資料庫密碼。
- --database-host 值符合主要應用裝置的 eth1 網路 IP 位址。
- --keystore 值是您在步驟 10.b 中備份的 certificates.ks 檔案的路徑。
- --primary-ip 值符合應用裝置的 eth0 網路 IP 位址。
- --console-proxy-ip 值符合應用裝置的 eth0 網路 IP 位址。

如需疑難排解資訊，請參閱[移轉或還原到 vCloud Director 應用裝置時重新設定 vCloud Director 服務失敗](#)。

- d 執行命令以啟動 vCloud Director 服務。

```
service vmware-vcd start
```

您可以在 /opt/vmware/vcloud-director/logs/cell.log 中監控儲存格的啟動進度。

- 11 在新伺服器群組的所有儲存格完成啟動程序後，確認 vCloud Director 環境已成功移轉。
  - a 使用新伺服器群組中任意儲存格的 eth0 網路 IP 位址 (即 `https://et0_IP_new_cell/cloud`)，開啟 vCloud Director Web Console。
  - b 使用現有的**系統管理員**認證登入 vCloud Director Web Console。
  - c 驗證您的 vSphere 和雲端資源在新環境中是否可用。
- 12 成功驗證 vCloud Director 移轉之後，使用 vCloud Director Web Console 刪除屬於舊 vCloud Director 環境的已中斷連線的儲存格。
  - a 從**管理與監視**索引標籤，按一下**雲端儲存格**。
  - b 在儲存格名稱上按一下滑鼠右鍵，然後選取**刪除**。

您可以部署 vCloud Director 應用裝置，以將成員新增至移轉環境中的伺服器群組。

## 後續步驟

新移轉的 vCloud Director 應用裝置環境使用自我簽署憑證。若要在新環境的每個儲存格上使用舊環境中妥善簽署的憑證，請遵循下列步驟進行操作：

- 1 將舊儲存格中的金鑰儲存區檔案複製到 `/opt/vmware/vcloud-director/data/transfer/certificates.ks` 並取代。
- 2 執行儲存格管理工具命令以取代憑證。

確保 `vcloud.vcloud` 是此檔案的擁有者。

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

- 3 重新啟動 vCloud Director 服務。

```
service vmware-vcd restart
```

如果您將新成員新增到此伺服器群組，將使用這些妥善簽署的憑證部署新的應用裝置儲存格。

## 將使用外部 PostgreSQL 資料庫的 vCloud Director 移轉到 vCloud Director 應用裝置

如果更早版本的目前 vCloud Director 環境使用外部 PostgreSQL 資料庫，您可以移轉到包含 vCloud Director 9.7 應用裝置部署的新 vCloud Director 環境。您目前的 vCloud Director 環境可以包含 Linux 上的 vCloud Director 安裝或 vCloud Director 應用裝置部署。新的 vCloud Director 環境可以在高可用性模式下使用應用裝置的內嵌式 PostgreSQL 資料庫。

移轉工作流程包括四個主要階段。

- 升級現有 vCloud Director 環境
- 透過部署 vCloud Director 9.7 應用裝置的一或多個執行個體，建立新的 vCloud Director 伺服器群組
- 將外部資料庫移轉至內嵌式資料庫
- 複製共用傳輸服務資料和憑證資料。

### 程序

- 1 如果您目前的外部 PostgreSQL 資料庫版本為 9.x，請將外部 PostgreSQL 資料庫升級至 10 版。
- 2 將目前的 vCloud Director 環境升級到 9.7 版。  
請參閱 [第 11 章 升級 vCloud Director 和修補 vCloud Director 應用裝置](#)。
- 3 確認移轉來源 vCloud Director 重新啟動成功。
- 4 在升級後的 vCloud Director 環境的每個儲存格上，執行命令以停止 vCloud Director 服務。

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

- 5 在外部 PostgreSQL 資料庫上，備份目前資料庫。

```
sudo -u postgres path_to_pg_dump -Fc db_name > /tmp/db_dump_name
```

如果 `/tmp` 資料夾上沒有足夠的可用空間，請使用其他位置來儲存傾印檔案。

- 6 如果資料庫擁有者和資料庫名稱不是 `vcloud`，請記下此使用者名稱和資料庫名稱。  
在步驟 13 中，您必須在新環境中建立此使用者並重新命名資料庫。
- 7 如果您希望新的 vCloud Director 環境使用現有環境的 IP 位址，則必須將內容和憑證檔案複製到外部 PostgreSQL 資料庫上的某個位置，然後關閉儲存格電源。
- 將位於 `/opt/vmware/vcloud-director/etc/` 的 `global.properties`、`responses.properties`、`certificates` 和 `proxycertificates` 檔案複製到 `/tmp` 或外部 PostgreSQL 資料庫上的任何慣用位置。
  - 將現有環境中的儲存格關閉電源。
- 8 如果您想讓新 vCloud Director 環境使用現有環境的 NFS 伺服器，請建立並匯出此 NFS 伺服器上的新目錄做為新的共用 NFS 掛接點。  
您無法重複使用現有的掛接點，因為舊 NFS 中使用者的使用者識別碼和群組識別碼 (UID/GID) 可能與新 NFS 中的使用者識別碼和群組識別碼不相符。
- 9 透過部署 vCloud Director 9.7 應用裝置的一或多個執行個體，建立新的伺服器群組。
- 如果您想要使用資料庫高可用性功能，則部署一個主要儲存格和兩個待命儲存格，並選擇性地部署一或多個 vCD 應用程式儲存格。
  - 如果已將現有環境中的儲存格關閉電源，您可以使用新儲存格的原始 IP 位址。
  - 如果已匯出現有 NFS 伺服器上的新路徑，您可以針對新環境使用這個新的共用掛接點。

請參閱第 6 章 [部署 vCloud Director 應用裝置](#)。

- 10 在每個新部署的儲存格上，執行命令以停止 vCloud Director 服務。

```
service vmware-vcd stop
```

- 11 將傾印檔案從外部 PostgreSQL 資料庫上的 `/tmp` 資料夾複製到新環境的主要儲存格上的 `/tmp` 資料夾中。

請參閱步驟 5。

- 12 變更傾印檔案的權限。

```
chmod a+r /tmp/db_dump_name
```

- 13 以 **root** 身分登入新部署的主要儲存格的主控台中，並將外部 vCloud Director 資料庫傳輸至內嵌式資料庫。

- 將使用者切換為 `postgres`，連線至 `psql` 資料庫終端機，然後執行捨棄 `vcloud` 資料庫的陳述式。

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

- b 如果現有外部資料庫的資料庫擁有者不是 `vcloud`，請使用您在步驟 6 中記下的名稱建立一個使用者。

```
sudo -i -u postgres /opt/vmware/vpostgres/current/bin/psql -c 'CREATE USER
<db_owner_external_pg>;'
```

- c 執行 `pg_restore` 命令。

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

- d 如果現有外部資料庫的資料庫擁有者不是 `vcloud`，請使用您在步驟 6 中記下的名稱將資料庫名稱變更為 `vcloud`。

```
sudo -i -u postgres /opt/vmware/vpostgres/current/bin/psql -c 'ALTER DATABASE
<db_name_external_pg> RENAME TO vcloud;'
```

- e 如果現有 vCloud Director 環境的資料庫擁有者不是 `vcloud`，請將資料庫擁有者變更為 `vcloud`，並將資料表重新指派給 `vcloud`。

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

```
sudo -i -u postgres /opt/vmware/vpostgres/current/bin/psql -d vcloud -c 'REASSIGN OWNED BY
<db_owner_external_pg> TO vcloud;'
```

- 14 在每個新部署的儲存格上，備份和取代組態資料，然後重新設定並啟動 vCloud Director 服務。

- a 備份內容和憑證檔案，然後從移轉來源的外部 PostgreSQL 資料庫上的位置 (在步驟 7a 中將檔案複製到的位置) 複製並取代這些檔案。

`global.properties`、`responses.properties`、`certificates` 和 `proxycertificates` 檔案位於 `/opt/vmware/vcloud-director/etc/`。

**重要** 如果您要移轉至 vCloud Director 版本 9.7.0.1 或更新版本，還必須備份、複製和取代移轉來源中的 `truststore` 檔案以及其他檔案。

- b 備份 `/opt/vmware/vcloud-director/certificates.ks` 中的金鑰儲存區檔案。

請勿從移轉來源複製和取代為金鑰儲存區檔案。

- c 執行命令以重新設定 vCloud Director 服務。

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

其中：

- `--keystore-password` 值符合此應用裝置的初始 **root** 密碼。
- `--database-password` 值符合您在應用裝置部署期間設定的資料庫密碼。
- `--database-host` 值符合主要應用裝置的 `eth1` 網路 IP 位址。
- `--primary-ip` 值符合應用裝置的 `eth0` 網路 IP 位址。
- `--console-proxy-ip` 值符合應用裝置的 `eth0` 網路 IP 位址。
- `--console-proxy-port` 值符合應用裝置主控台 Proxy 連接埠 8443。

如需疑難排解資訊，請參閱[移轉或還原到 vCloud Director 應用裝置時重新設定 vCloud Director 服務失敗](#)。

- d 執行命令以啟動 vCloud Director 服務。

```
service vmware-vcd start
```

您可以在 `/opt/vmware/vcloud-director/logs/cell.log` 中監控儲存格的啟動進度。

- 15 在新伺服器群組的所有儲存格完成啟動程序後，確認 vCloud Director 環境已成功移轉。
  - a 使用新伺服器群組中任意儲存格的 `eth0` 網路 IP 位址 (即 `https://et0_IP_new_cell/cloud`)，開啟 vCloud Director Web Console。
  - b 使用現有的**系統管理員**認證登入 vCloud Director Web Console。
  - c 驗證您的 vSphere 和雲端資源在新環境中是否可用。
- 16 成功驗證 vCloud Director 移轉之後，使用 vCloud Director Web Console 刪除屬於舊 vCloud Director 環境的已中斷連線的儲存格。
  - a 從**管理與監視**索引標籤，按一下**雲端儲存格**。
  - b 在儲存格名稱上按一下滑鼠右鍵，然後選取**刪除**。

您可以部署 vCloud Director 應用裝置，以將成員新增至移轉環境中的伺服器群組。

## 後續步驟

新移轉的 vCloud Director 應用裝置環境使用自我簽署憑證。若要在新環境的每個儲存格上使用舊環境中妥善簽署的憑證，請遵循下列步驟進行操作：

- 1 將舊儲存格中的金鑰儲存區檔案複製到 `/opt/vmware/vcloud-director/data/transfer/certificates.ks` 並取代。
- 2 執行儲存格管理工具命令以取代憑證。

確保 `vcloud.vcloud` 是此檔案的擁有者。

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

### 3 重新啟動 vCloud Director 服務。

```
service vmware-vcd restart
```

如果您將新成員新增到此伺服器群組，將使用這些妥善簽署的憑證部署新的應用裝置儲存格。

# 升級或移轉 vCloud Director 之後

# 13

升級或移轉所有 vCloud Director 伺服器 and 共用資料庫後，您可以升級為雲端提供網路服務的 NSX Manager 執行個體。然後，可以升級已登錄至 vCloud Director 安裝的 ESXi 主機和 vCenter Server 執行個體。

---

**重要** 從 9.7 版開始，vCloud Director 僅支援進階 Edge 閘道。您必須將任何舊版非進階 Edge 閘道轉換為進階閘道。請參閱 <https://kb.vmware.com/kb/66767>。

---

本章節討論下列主題：

- 升級與已連接 vCenter Server 系統相關聯的每個 NSX Manager
- 升級 vCenter Server 系統、ESXi 主機和 NSX Edge
- 此版本中的新權限

## 升級與已連接 vCenter Server 系統相關聯的每個 NSX Manager

升級登錄到 vCloud Director 的 vCenter Server 和 ESXi 主機之前，您必須升級與此 vCenter Server 相關聯的每個 NSX Manager。

升級 NSX Manager 會中斷 NSX 管理功能的存取，但是不會中斷網路服務。您可以在升級 vCloud Director 之前或之後升級 NSX Manager，無論是否有任何 vCloud Director 儲存格正在執行。

如需升級 NSX 的相關資訊，請參閱 NSX for vSphere 說明文件，網址為 <https://docs.vmware.com>。

### 程序

- 1 升級與登錄到 vCloud Director 安裝的每個 vCenter Server 相關聯的 NSX Manager。
- 2 升級所有 NSX Manager 之後，您可以升級已登錄的 vCenter Server 系統和 ESXi 主機。

## 升級 vCenter Server 系統、ESXi 主機和 NSX Edge

升級 vCloud Director 和 NSX Manager 後，您必須升級已登錄至 vCloud Director 的 vCenter Server 系統和 ESXi 主機。升級所有已連結的 vCenter Server 系統和 ESXi 主機後，您可以升級 NSX Edge。

### 必要條件

請確認您已升級與連結至雲端之 vCenter Server 系統相關聯的每個 NSX Manager。請參閱[升級與已連接 vCenter Server 系統相關聯的每個 NSX Manager](#)。

## 程序

### 1 停用 vCenter Server 執行個體。

- a 在 vCloud Director Web 主控台中，按一下**管理與監視**索引標籤，然後在左窗格中按一下**vCenter**。
- b 在目標 vCenter Server 名稱上按一下滑鼠右鍵，然後按一下**停用**。
- c 按一下**是**。

### 2 升級 vCenter Server 系統。

如需相關資訊，請參閱《vCenter Server 升級》。

### 3 驗證所有 vCloud Director 公用 URL 和憑證鏈結。

- a 在 vCloud Director Web 主控台中，按一下**管理**索引標籤，然後在左窗格中按一下**公用位址**。
- b 確認所有公用位址。

### 4 重新整理 vCenter Server 向 vCloud Director 的登錄。

- a 在 vCloud Director Web 主控台中，按一下**管理與監視**索引標籤，然後在左窗格中按一下**vCenter**。
- b 在目標 vCenter Server 名稱上按一下滑鼠右鍵，然後按一下**重新整理**。
- c 按一下**是**。

### 5 升級已升級的 vCenter Server 系統所支援的每台 ESXi 主機。

請參閱《VMware ESXi 升級》。

---

**重要** 若要確定您有足夠的已升級主機容量可支援雲端中的虛擬機器，請以小批次的方式升級主機。當您這樣做時，主機代理程式升級可以及時完成，以允許虛擬機器移轉回到已升級的主機。

---

- a 使用 vCenter Server 系統將主機置於維護模式，並允許該主機上的所有虛擬機器移轉至另一台主機。
  - b 升級主機。
  - c 使用 vCenter Server 系統重新連線主機。
  - d 使用 vCenter Server 系統讓主機退出維護模式。
- ### 6 (選擇性) 升級與已升級 vCenter Server 系統相關聯之 NSX Manager 所管理的 NSX Edge。
- 已升級的 NSX Edge 在效能和整合方面有所改進。您可以使用 NSX Manager 或 vCloud Director 升級 NSX Edge。
- 如需使用 NSX Manager 升級 NSX Edge 的相關資訊，請參閱 NSX for vSphere 說明文件，網址為 <https://docs.vmware.com>。

- 若要使用 vCloud Director 升級 NSX Edge，您必須在 Edge 支援的 vCloud Director 網路物件上操作：
  - 當您使用 vCloud Director Web 主控台或 vCloud API 重設 Edge 閘道所服務的網路時，會自動適當地升級 Edge 閘道。
  - 重新部署 Edge 閘道會升級相關聯的 NSX Edge 應用裝置。
  - 從 vApp 環境中重設 vApp 網路時，會升級與此網路相關聯的 NSX Edge 應用裝置。若要使用 vCloud Director Web 主控台從 vApp 的環境內重設 vApp 網路，請導覽到 vApp 的網路索引標籤、顯示其網路詳細資訊、在 vApp 網路上按一下滑鼠右鍵，然後選取**重設網路**。

如需有關如何重新部署 Edge 閘道和重設 vApp 網路的詳細資訊，請參閱 vCloud Director Web 主控台線上說明或《vCloud API 程式設計指南》。

### 後續步驟

對已登錄至 vCloud Director 安裝的其他 vCenter Server 系統重複此程序。

## 此版本中的新權限

vCloud Director 9.7 採用了新權限，您可能想要將這些權限新增至發佈到您的承租人的任何現有全域角色。

權限	描述	預設角色
<b>SDDC：檢視 SDDC</b>	可讓您檢視向您的組織發佈的所有 SDDC。 系統管理員可以檢視所有 SDDC。	系統管理員和組織管理員
<b>SDDC：管理 SDDC</b>	可讓您新增、移除和編輯 SDDC。	系統管理員
<b>SDDC：管理 SDDC Proxy</b>	可讓您新增、移除、啟用及停用 SDDC Proxy。	系統管理員
<b>服務應用程式：檢視服務應用程式</b>	可讓您查看已登錄的服務應用程式的清單。 用於 VMC 帳戶。	系統管理員
<b>服務應用程式：登錄 VMC SDDC</b>	可讓您建立、檢視、編輯和移除服務應用程式。 用於 VMC 帳戶。	系統管理員
<b>服務應用程式：管理服務應用程式</b>	可讓您登錄服務應用程式。 用於 VMC 帳戶。	系統管理員
<b>Edge 叢集：檢視 Edge 叢集</b>	可讓您查看 Edge 叢集的清單並擷取個別 Edge 叢集。	系統管理員和組織管理員
<b>Edge 叢集：管理 Edge 叢集</b>	可讓您建立、編輯和移除 Edge 叢集。	系統管理員和組織管理員
<b>vApp：編輯虛擬機器運算原則</b>	允許使用者變更虛擬機器的運算原則。	系統管理員、組織管理員、目錄作者和 vApp 作者
<b>閘道：匯入 Edge 閘道</b>	可讓您匯入第 1 層路由器做為 Edge 閘道。	系統管理員和組織管理員

如需管理權限和角色的相關資訊，請參閱《vCloud Director Service Provider Admin Portal 指南》。

如果 vCloud Director 應用裝置部署失敗，或應用裝置未正常運作，您可以檢查應用裝置記錄檔以判斷問題的原因。

VMware 技術支援通常在處理支援請求時要求提供診斷資訊。您可以使用 `vmware-vcd-support` 指令碼收集主機記錄資訊和 vCloud Director 記錄。如需有關收集 vCloud Director 的診斷資訊的詳細資訊，請參閱 <https://kb.vmware.com/s/article/1026312>。執行 `vmware-vcd-support` 指令碼時，記錄可能包含已解除委任或已取代的儲存格 (狀態為失敗) 的相關資訊。請參閱 <https://kb.vmware.com/s/article/71349>。

本章節討論下列主題：

- [檢查 vCloud Director 應用裝置中的記錄檔](#)
- [vCloud Director 儲存格在應用裝置部署後無法啟動](#)
- [移轉或還原到 vCloud Director 應用裝置時重新設定 vCloud Director 服務失敗](#)
- [使用記錄檔對 vCloud Director 更新和修補程式進行疑難排解](#)
- [檢查 vCloud Director 更新失敗](#)
- [安裝 vCloud Director 的最新更新失敗](#)

## 檢查 vCloud Director 應用裝置中的記錄檔

部署 vCloud Director 應用裝置後，您可以檢查首次開機和資料庫記錄中的錯誤和警告。

### 程序

- 1 以 **root** 身分直接登入或使用 SSH 登入 vCloud Director 應用裝置主控台。
- 2 導覽至 `/opt/vmware/var/log`。
- 3 檢查記錄檔。
  - `firstboot` 檔案包含與應用裝置首次開機相關的記錄資訊。
  - `/opt/vmware/var/log/vcd/` 目錄包含與 Replication Manager (repmgr) 工具套件安裝、重新設定和應用裝置同步相關的記錄。
  - `/opt/vmware/var/log/vcd/pg/` 目錄包含與內嵌式應用裝置資料庫的備份相關的記錄。
  - `/opt/vmware/etc/vami/ovfEnv.xml` 檔案包含部署 OVF 參數。

## vCloud Director 儲存格在應用裝置部署後無法啟動

您已成功部署 vCloud Director 應用裝置，但 vCloud Director 服務可能無法啟動。

### 問題

vmware-vcd 服務在應用裝置部署後處於非作用中狀態。

### 原因

如果已部署主要儲存格，vCloud Director 服務可能因為預先填入的 NFS 共用傳輸服務儲存區而無法啟動。部署主要應用裝置之前，共用傳輸服務儲存區不得包含 `responses.properties` 檔案或 `appliance-nodes` 目錄。

如果已部署待命儲存格或 vCD 應用程式儲存格，vCloud Director 服務可能無法啟動，因為 NFS 共用傳輸儲存區中遺失 `responses.properties` 檔案。部署待命應用裝置或 vCD 應用程式應用裝置之前，共用傳輸服務儲存區必須包含 `responses.properties` 檔案。

### 解決方案

- 1 以 **root** 身分直接登入或使用 SSH 登入 vCloud Director 應用裝置主控台。
- 2 檢查 `/opt/vmware/var/log/vcd/setupvcd.log` 中有關 NFS 儲存區的錯誤訊息。
- 3 針對應用裝置類型準備 NFS 儲存區。
- 4 重新部署儲存格。

## 移轉或還原到 vCloud Director 應用裝置時重新設定 vCloud Director 服務失敗

移轉或還原到 vCloud Director 應用裝置時，執行 `configure` 命令可能會失敗。

### 問題

執行將 vCloud Director 移轉或還原到新的 vCloud Director 應用裝置環境的程序期間，您可以執行 `configure` 命令以重新設定每個新儲存格中的 vCloud Director 服務。`configure` 命令可能會失敗並顯示錯誤訊息 `sun.security.validator.ValidatorException: PKIX 路徑驗證失敗`：  
`java.security.cert.CertPathValidatorException: 簽章檢查失敗`。

### 解決方案

- 1 在目標儲存格上執行命令。

```
sed -i '/vcd_ova.crt/ s/$/ --force /' /opt/vmware/appliance/bin/appliance-sync.sh
```

- 2 等待 1 分鐘，然後重新執行 `configure` 命令。

## 使用記錄檔對 vCloud Director 更新和修補程式進行疑難排解

將修補程式套用到 vCloud Director 應用裝置時，您可以檢查記錄檔中是否存在錯誤和警告。

## 問題

如果 `vamicli` 命令傳回錯誤，您可以使用記錄檔進行疑難排解。

## 解決方案

- 1 以 **root** 身分直接登入或使用 SSH 登入 vCloud Director 應用裝置主控台。
- 2 導覽至相應的記錄檔。
  - 如果 `vamicli update --check` 失敗，請導覽至 `/opt/vmware/var/log/vami/vami.log`。
  - 如果 `vamicli update --install latest` 失敗，請導覽至 `/opt/vmware/var/log/vami/updatecli.log`。
- 3 檢查記錄檔。

## 檢查 vCloud Director 更新失敗

檢查 vCloud Director 應用裝置的更新時，執行 `vamicli update --check` 命令可能會失敗。

## 問題

將修補程式套用至 vCloud Director 應用裝置的程序期間，您可以執行 `vamicli update --check` 命令以檢查是否有可用更新。`vamicli update --check` 命令可能會失敗並顯示失敗：下載資訊清單時發生錯誤。請連絡廠商。

## 原因

更新存放庫目錄的路徑不正確。

## 解決方案

- 1 使用正確的路徑執行 `vamicli` 命令。

```
vamicli update --repo file:/root/local-update-repo
```

- 2 再次執行命令以檢查是否有更新。

```
vamicli update --check
```

## 安裝 vCloud Director 的最新更新失敗

安裝 vCloud Director 應用裝置的最新更新時，執行 `vamicli update --install latest` 命令可能會失敗。

## 問題

將修補程式套用至 vCloud Director 應用裝置的程序期間，您可以執行 `vamicli update --install latest` 命令以套用最新的可用修補程式。`vamicli update --install latest` 命令可能會失敗並顯示失敗：執行套件安裝時發生錯誤

## 原因

當 NFS 伺服器無法存取時，就會發生此錯誤。

## 解決方案

- 1 確認掛接到 `/opt/vmware/vcloud-director/data/transfer` 的 NFS 伺服器可供存取。
- 2 再次執行命令以套用可用的修補程式。

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

# 解除安裝 vCloud Director 軟體

# 15

使用 Linux rpm 命令，從個別伺服器解除安裝 vCloud Director 軟體。

## 程序

- 1 以**根使用者**身分登入目標伺服器。
- 2 卸載傳輸服務儲存空間，通常裝載於 `/opt/vmware/vcloud-director/data/transfer`。
- 3 開啟主控台、Shell 或終端機視窗，然後執行 Linux rpm 命令。

```
rpm -e vmware-phonhome vmware-vcloud-director vmware-vcloud-director-rhel
```

如果其他已安裝的套件依賴 `vmware-vcloud-director` 套件，系統會提示您在解除安裝 vCloud Director 前先解除安裝這些套件。