

VMware Cloud Director 10.1 版本說明

VMware Cloud Director 10.1 | 2020 年 4 月 9 日 | 組建編號 15967253 (已安裝的組建編號 15967236)

查看這些版本說明的新增項目和更新。

本文件的内容

- [此版本的新增功能](#)
- [安全性](#)
- [產品支援通知](#)
- [從先前版本升級](#)
- [系統需求與安裝](#)
- [已解決的問題](#)
- [已知問題](#)

此版本的新增功能

- 如需此版本之新增功能和更新功能的相關資訊，請參閱 VMware 技術白皮書 [《VMware vCloud Director 10.1 的新增功能》](#)。
- 已變更 HTML5 使用者介面中的行為：
在舊版 VMware Cloud Director 中，您可以使用 HTML 使用者介面中的 vApp 動作功能表來停止或關閉 vApp 的電源。這兩個電源作業都會取消部署 vApp，但會以不同方式影響 vApp。關閉電源作業不會遵循 vApp 中虛擬機器的 [開始和停止順序] 設定。關閉電源作業也會將所有虛擬機器 NIC 與組織 VDC 網路中斷連線，並移除為 vApp 部署的任何 Edge 閘道，以取消部署任何 vApp 網路。

在 VMware Cloud Director 10.1 中，對執行中的 vApp 執行關閉電源作業會導致關閉 vApp 中所有虛擬機器的電源，而不會取消部署 vApp 和其中的虛擬機器。虛擬機器的 NIC 仍保持連線到相應的網路，且任何 vApp Edge 閘道仍會保持部署狀態。vApp 和 vApp 中的虛擬機器仍會保持部署狀態。vApp 中每個個別虛擬機器的關閉電源動作會保持作用中狀態，您可以使用此動作關閉虛擬機器的電源。此動作會導致取消部署此虛擬機器。

當您關閉 vApp 電源時，關閉電源作業會遵循您在 [開始和停止順序] 設定中定義的開始順序。因此，會按照為虛擬機器設定的開始順序相反的順序關閉虛擬機器的電源。在關閉電源作業期間不會套用 [停止等候] 設定。當您關閉 vApp 的電源時，vApp 的電源狀態 (衍生自其中虛擬機器的電源狀態) 會顯示為 [已關閉電源]。

- VMware Cloud Director API 34.0 架構包含 numberOfCpus 和 MemoryAllocationMB 屬性的定義。

安全性

- **警告：**升級至版本 10.1 後，VMware Cloud Director 將一律驗證與其連線的任何基礎結構端點的憑證。這是因為 VMware Cloud Director 管理 SSL 憑證的方式有所變更。如果您在升級前未將憑證匯入至 VMware Cloud Director，由於 SSL 驗證問題，vCenter Server 和 NSX 連線可能會顯示連線失敗錯誤。在此情況下，升級後有兩個選項可用：
 1. 執行儲存格管理工具 `trust-infra-certs` 命令，自動將 vCenter Server 和 NSX Manager 執行個體之所有基礎結構端點的憑證連線並擷取至集中式憑證存放區。請參閱 [〈從 vSphere 資源匯入端點憑證〉](#)。
 2. 在服務提供者管理入口網站使用者介面中，選取每個 vCenter Server 和 NSX 執行個體，然後在接受憑證時重新輸入認證。
- 從 10.1 版開始，服務提供者和承租人可使用 VMware Cloud Director API 測試與遠端伺服器的連線，並在 SSL 信號交換過程中驗證伺服器身分識別。若要保護 VMware Cloud Director 網路連線，請為使用 VMware Cloud Director API 進行連線測試的承租人設定其無法連線的內部主機的封鎖清單。請在 VMware Cloud Director 安裝或升級之後，在向 VMware Cloud Director 授與承租人存取權之前設定封鎖清單。請參閱 [〈設定測試連線封鎖清單〉](#)。
- 在 VMware Cloud Director 10.1 中，取代了信任所有 SSL 憑證的行為。在此版本中，vCenter Server 和 NSX 連線不支援此選項。對於所有其他連線，信任所有憑證也會被取代，在 VMware Cloud Director 10.1 之後將不再受支援。系統管理員必須為此轉換做好準備。
 - 如果針對 VMware Cloud Director 系統組織使用 LDAP，您可以使用使用者介面中的 [首次使用時信任] 對話方塊，或使用 API 上傳憑證。
 - 對此選項的所有使用情況進行稽核，並透過使用使用者介面或 API 提供適當的憑證。
 - 將變更傳達給承租人。使用已啟用**接受所有憑證**選項之自訂 LDAP 的所有承租人，都必須從此組態進行轉換。承租人可以使用使用者介面中的 [首次使用時信任] 對話方塊，或透過 API 上傳憑證。

更新的開放原始碼套件

- 已將 `jackson-databind` 更新至版本 2.9.10.1。
- 已將 `jre` 更新至版本 1.8.0u231。
- 已將 `openssl` 更新至版本 1.0.2u。
- 已將 `xstream` 更新至版本 1.4.11.1。

產品支援通知

VMware Cloud Director 10.1 不支援 vSphere 7.0 和 NSX-T Data Center 3.0。正在進行互通性認證，在 VMware Cloud Director 10.1 的次要修補程式發行版本中將支援 vSphere 7.0 和 NSX-T Data Center 3.0。

不支援 NSX-T Data Center 中 VRF-lite 第 0 層閘道所支援的外部網路。

生命週期和支援結束警告

- 不再支援 SQL Server 資料庫。僅支援 PostgreSQL 資料庫。

- 不再支援 Oracle Linux 作為安裝 VMware Cloud Director 應用程式的主機作業系統。
- 不支援 VMware Cloud Director API 版本 20 及更早版本。
- VMware Cloud Director API 版本 27.0 - 29.0 已被取代，並且在 VMware Cloud Director 10.1 之後將不再受支援
- VMware Cloud Director API 版本 30.0 已被取代。
- 以 Flex 為基礎的使用者介面已從產品中移除，且不再受支援。
- 在 VMware Cloud Director API 版本 33.0/VMware Cloud Director 10.0 中，/api/sessions API 登入端點已被取代，並且在未來的 VMware Cloud Director 版本中將不受支援。您可以使用單獨的 VMware Cloud Director OpenAPI 登入端點，以供服務提供者和承租人存取 VMware Cloud Director。
- HTTP 和 HTTPS 通訊協定的 API /cloud/server_status 已被取代，並且將在未來版本中移除。必須針對 HTTP 和 HTTPS 通訊協定使用 /api/server_status。
- 由於 VMware Cloud Director 10.1 儲存和處理 SSL 憑證的方式，/ldap/action/resetLdapCertificate 和 /ldap/action/resetLdapKeyStore 重設動作已從 VMware Cloud Director API 版本 34.0 中移除。您必須使用 /cloudapi/1.0.0/ssl/trustedCertificates 端點來取消信任憑證。
- /ldap/action/updateLdapCertificate 和 /ldap/action/updateLdapKeyStore 更新動作已被取代，並且在未來版本中將不受支援。VMware Cloud Director 引入了新端點用於信任 LDAP 憑證 /cloudapi/1.0.0/ssl/trustedCertificates。
- vSphere 取代 vSphere SSO 作為 SAML IDP。設定為使用 vSphere SSO 作為其 SAML IDP 的所有 VMware Cloud Director 部署，都必須移轉至其他外部 SAML IDP。在未來的 vSphere 和 VMware Cloud Director 版本中將不支援使用此 IDP。
- 由於沒有建議的加密套件可供使用，因此不再支援 DSA 和 DSS 憑證。

即將結束支援注意事項

- VMware Cloud Director API 34.0 (VMware Cloud Director 10.1) 包含正在加速取代且將在未來版本中移除的 API。請參閱 [《VMware Cloud Director API 程式設計指南》](#)。

從先前版本升級

如需有關升級至 VMware Cloud Director 10.1、升級和移轉路徑和工作流程的詳細資訊，請參閱 [〈升級和移轉 VMware Cloud Director 應用裝置〉](#) 或 [〈在 Linux 上升級 vCloud Director〉](#)。

系統需求與安裝

連接埠和通訊協定

如需 VMware Cloud Director 10.1 所使用的網路連接埠和通訊協定的相關資訊，請參閱 [〈VMware 連接埠和通訊協定〉](#)。

相容性矩陣圖

請參閱 [《VMware 產品互通性對照表》](#)，以瞭解關於下列內容的最新資訊：

- VMware Cloud Director 與其他 VMware 平台的互通性
- 支援的 VMware Cloud Director 資料庫

支援的 VMware Cloud Director 伺服器作業系統

- CentOS 6
- CentOS 7
- Red Hat Enterprise Linux 6
- Red Hat Enterprise Linux 7

支援的 AMQP 伺服器

VMware Cloud Director 會使用 AMQP 來提供由延伸服務、物件延伸及通知所使用的訊息匯流排。此版本的 VMware Cloud Director 需要 RabbitMQ 版本 3.7.9 或 3.8.2

如需詳細資訊，請參閱《VMware Cloud Director 安裝、設定與升級指南》。

用於儲存歷史度量資料的受支援資料庫

您可以設定 VMware Cloud Director 安裝以儲存 VMware Cloud Director 收集之關於虛擬機器效能和資源耗用量的度量。歷史度量資料儲存在 Cassandra 資料庫中。VMware Cloud Director 支援 Cassandra 版本 3.x。

如需詳細資訊，請參閱《VMware Cloud Director 安裝、設定與升級指南》。

磁碟空間需求

每一個 VMware Cloud Director 伺服器需要大約 2100 MB 的可用空間，供安裝及記錄檔使用。

記憶體需求

請參閱《VMware Cloud Director 安裝、設定與升級指南》以瞭解記憶體需求

CPU 需求

VMware Cloud Director 是一種 CPU 繫結的應用程式。應遵循適當 vSphere 版本的 CPU 過度認可準則。在虛擬化環境中，不論 VMware Cloud Director 可用的核心數為何，都必須具有合理的 vCPU 與實體 CPU 比率，以免造成極端的過度認可。

必要的 Linux 軟體套件

每一個 VMware Cloud Director 伺服器必須包括數個常用 Linux 軟體套件的安裝。依預設，這些套件會與作業系統軟體一起安裝。如果有任何套件遺失，則安裝程式會失敗並顯示診斷訊息。

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

除了安裝程式所需的套件外，數個設定網路連線並建立 SSL 憑證的程序需要使用 Linux bind-utils 套件中提供的 Linux nslookup 命令。

支援的 LDAP 伺服器

您可以從下列 LDAP 服務將使用者和群組匯入至 VMware Cloud Director。

平台	LDAP 服務	驗證方法
Windows Server 2012	Active Directory	簡單, 簡單 SSL
Windows Server 2016	Active Directory	簡單, 簡單 SSL
Linux	OpenLDAP	簡單, 簡單 SSL

支援的安全性通訊協定及加密套件

VMware Cloud Director 要求用戶端連線是安全的。SSL 版本 3 和 TLS 版本 1.0 與 1.1 經發現存在嚴重的安全性漏洞，已不再包含於伺服器在進行用戶端連線時提供使用的一組預設通訊協定中。系統管理員可啟用更多通訊協定和加密套件。請參閱《VMware Cloud Director 安裝、設定與升級指南》中的〈儲存格管理工具〉一節。支援下列安全性通訊協定：

- TLS 1.2 版
- TLS 1.1 版 (依預設為停用)
- TLS 1.0 版 (依預設為停用)

預設會啟用的支援加密套件：

- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

系統管理員可使用儲存格管理工具，以明確啟用預設已停用的其他支援加密套件。

備註：與低於 5.5-update-3e 之 vCenter Server 版本及低於 4.2 之 ovftool 版本互通要求 VMware Cloud Director 支援 TLS 1.0 版。您可以使用儲存格管理工具重新設定一組支援的 SSL 通訊協定或加密方式。請參閱《VMware Cloud Director 安裝、設定與升級指南》中的〈儲存格管理工具〉一節。

支援的瀏覽器

VMware Cloud Director 與下列瀏覽器的目前主要版本和上一個主要版本相容：

- Google Chrome
- Mozilla Firefox
- Microsoft Edge
- Microsoft Internet Explorer 11

支援的客體作業系統與虛擬硬體版本

對於支援每個資源集區的 ESXi 主機，VMware Cloud Director 支援此類主機所支援的所有客體作業系統和虛擬硬體版本。

VMware Cloud Director WebMKS 2.1.1

VMware Cloud Director WebMKS 2.1.1 主控台新增了以下支援：

- Google Chrome 和適用於 Windows 的 Mozilla Firefox 中的 PrintScreen 鍵。
- Windows 和 macOS 中的 Windows 鍵。若要模擬按 Windows 鍵，請在 Windows 作業系統中按 Ctrl+Windows，或在 macOS 中按 Ctrl+Command。
- Google Chrome 和 Mozilla Firefox 中的自動鍵盤配置偵測。

已解決的問題

- **當您關聯兩個 VMware Cloud Director 應用裝置站台時，無法在站台中看到物件**
如果要關聯站台並且您的站台具有組織、組織 VDC、vApp、虛擬機器等物件，則無法看到目前站台中的物件。HTML 5 使用者介面僅顯示其他相關聯站台中的物件。在多站台扇出通訊期間會發生此問題，因為 VMware Cloud Director 應用裝置的 /etc/hosts 檔案中沒有正確的內容。
- **更新虛擬機器大小調整原則失敗，並顯示記憶體配置錯誤**
如果您將配置集區 VDC 轉換為彈性組織 VDC，vCloud Director 會在轉換前保留來自配置集區 VDC 的最大原則資訊。高於配置集區 VDC 中定義之保留的 CPU 或記憶體保留保證失敗，並顯示虛擬機器保留、限制或共用率設定無效錯誤。
- **在多儲存格環境中，靜止或暫停主要儲存格不會在次要儲存格上重新啟動定期工作**
在多儲存格環境中，當您靜止或暫停主要儲存格時，不會從次要儲存格啟動在主要儲存格背景中執行的定期工作。
- **將已啟用資料服務的主機型儲存區原則上的虛擬機器複製到具有不同主機型儲存區原則的虛擬機器失敗，並顯示錯誤**

如果您建立的虛擬機器所在的儲存區原則已啟用 IOPS 或虛擬機器加密等主機型規則，則嘗試複製虛擬機器並變更目標虛擬機器的儲存區原則會失敗，並顯示錯誤在複製作業期間不允許變更或套用具有資料服務功能的虛擬機器儲存區原則。在複製作業完成後且虛擬機器開啟電源之前，可以將具有資料服務功能的虛擬機器儲存區原則指派給已佈建的虛擬機器。

- **全域承租人角色 vApp 作者可以上傳並建立範本和媒體，而無需執行這些作業的必要權限**
依預設，全域承租人角色 vApp 作者具有從我的雲端新增 vApp 權限。由於此權限和範本/媒體：建立/上傳權限共用單一作業，VMware Cloud Director 也會錯誤地向 vApp 作者角色授與範本/媒體：建立/上傳權限。

此問題已修正。如果您希望 vApp 作者角色繼續擁有範本/媒體：建立/上傳權限，服務提供者可以向 vApp 作者全域角色新增該權限並將其發佈到組織。

- **新建立的虛擬機器會部署在組織 VDC 預設儲存區原則上**
在 vCloud Director 租用戶入口網站中，當您建立新的獨立虛擬機器時，缺少用於指定儲存區原則的選項。因此，將使用組織 VDC 的預設儲存區原則來部署已建立的虛擬機器。

已知問題

- **新增 使用 Microsoft Internet Explorer 11 時無法開啟虛擬機器 Web 主控台**
使用 Microsoft Internet Explorer 11 連線至虛擬機器主控台會開啟空白視窗，無法存取虛擬機器主控台。
- **因應措施：**無。
- **新增 將保留集區 VDC 轉換為 Flex 組織 VDC 後，虛擬機器會變得不符合標準**
在具有保留集區配置模型的組織 VDC 中，如果某些虛擬機器的 CPU 和記憶體保留為非零和/或 CPU 和記憶體的組態為非無限制，則轉換為 Flex 組織 VDC 後，這些虛擬機器會變得不符合標準。如果嘗試讓虛擬機器再次符合標準，則系統會針對保留和限制套用不正確的原則，並將 CPU 和記憶體保留設定為零，以及將限制設定為**無限制**。

因應措施：

1. 系統管理員必須建立具有正確組態的虛擬機器大小調整原則。
 2. 系統管理員必須將新的虛擬機器大小調整原則發佈至轉換的 Flex 組織 VDC。
 3. 承租人可以使用 VMware Cloud Director API 或 VMware Cloud Director 租用戶入口網站，將虛擬機器大小調整原則指派給 Flex 組織 VDC 中的現有虛擬機器。
- **新增 在租用戶入口網站使用者介面中，當您建立相似性或反相似性規則時，取消選取 [必要] 核取方塊不會影響規則組態**
在租用戶入口網站使用者介面中，當您建立相似性或反相似性規則時，取消選取 [必要] 核取方塊不會影響規則組態。相似性和反相似性規則一律為 [必要]，這表示如果無法滿足規則，則新增至規則的虛擬機器將不會開啟電源。

因應措施：無。

- **新增 使用 VMware Cloud Director API 查詢 vApp 會針對 numberOfCpus 和 MemoryAllocationMB 屬性傳回空白欄位**

使用 VMware Cloud Director API 33.0 或更早版本執行 vApp REST API 查詢時，REST API 回應本文會針對 numberOfCpus 和 MemoryAllocationMB 屬性傳回空白欄位。發生此情況的原因是，API 架構不包括 numberOfCpus 和 MemoryAllocationMB 屬性的定義。

因應措施：使用 VMware Cloud Director API 34.0 查詢 vApp。

- **新增 嘗試將 NAT 規則新增至 NSX-T Edge 閘道失敗**

嘗試將 NAT 規則新增至 NSX-T Edge 閘道失敗，並顯示錯誤「已更新新值和已被取代的值以進行重新分配，錯誤碼 503266」。

因應措施：使用 NSX-T Data Center 原則 API 更新 NSX-T Edge 閘道連線之外部網路的重新分配組態。

1. 請記下支援 NSX-T Edge 閘道連線之外部網路的第 0 層路由器的識別碼。

- 執行 GET 要求以取得您環境中的第 0 層路由器的清單。

```
GET <nsxtmanagerurl>/policy/api/v1/infra/tier-0s
```

- 檢查清單以根據其顯示名稱識別第 0 層，該名稱與 VMware Cloud Director 使用者介面中外部網路的 [一般資訊] 索引標籤中的第 0 層路由器名稱相符。

2. 手動更新外部網路（第 0 層閘道）。

- 執行 GET 要求以取得路由器上 localeServices 的清單。

```
GET <nsxtmanagerurl>/policy/api/v1/infra/tier-0s/<TIER-0 ID>/locale-services
```

回應會傳回一個地區設定服務。

- 複製 localeService ID 並執行 GET 要求以進行檢查。

```
GET <nsxtmanagerurl>/policy/api/v1/infra/tier-0s/<TIER-0 ID>/locale-services/<LocaleServiceId>
```

回應會傳回地區設定服務的內容清單。

```
{
  "route_redistribution_config": {
    "bgp_enabled": true,
    "enabled": true,
    "redistribution_rules": [
      {
        "name": "some-name",
        "route_redistribution_types": [
          "TIER1_DNS_FORWARDER_IP",
          "TIER1_NAT",
          "TIER1_STATIC"
        ]
      }
    ]
  },
  ...
}
```

- 按如下所示修改回應。

```
{
  "route_redistribution_config": null,
  "route_redistribution_types": [
    "TIER1_DNS_FORWARDER_IP",
    "TIER1_NAT",
    "TIER1_STATIC"
  ]
}
```



```
],  
...  
}
```

- 使用修改後的內容執行 PUT 要求，以更新第 0 層路由器的 localeService。

- **新增** 如果目標儲存區容器為資料存放區叢集，將虛擬機器重新放置到其他叢集會失敗

如果您執行的作業導致嘗試將虛擬機器重新放置到其他叢集，而目標儲存區容器為資料存放區叢集，則移轉會失敗，並顯示 NO_FEASIBLE_PLACEMENT_SOLUTION 錯誤。在 VMware Cloud Director 記錄中，您會看到具有 invalidProperty = spec.host 的 Storage DRS 叫用錯誤。

因應措施：

1. 使用 vSphere Client 在目標資料存放區叢集上停用 Storage DRS，或使用 VMware Cloud Director API 將用於重新放置的目標儲存區變更為資料存放區。

2. 重新嘗試失敗的作業。

- **新增** 當您啟用在第一次登入時使 root 密碼到期的設定時，VMware Cloud Director 應用裝置部署會失敗

如果您嘗試部署已啟用在第一次登入時使 root 密碼到期設定的應用裝置，部署會失敗，且 /opt/vmware/var/log/firstboot 記錄檔會顯示錯誤：

```
[ERROR] postgresauth script failed to execute.
```

因應措施：停用在第一次登入時使 root 密碼到期設定，並指定至少包含八個字元，包括一個大寫字元、一個小寫字元、一個數字和一個特殊字元的初始 root 密碼。

- **新增** 當 vApp 使用者嘗試從範本建立 vApp 時，這可能會導致出現「操作被拒絕」訊息

如果您指派的使用者角色為 vApp 使用者，則當您嘗試從範本建立 vApp，並針對 vApp 中的虛擬機器自訂虛擬機器大小調整原則時，這會導致出現「操作被拒絕」訊息。發生此情況的原因是，vApp 使用者角色可讓您從範本具現化 vApp，但不包括允許您自訂虛擬機器記憶體、CPU 或硬碟的權限。透過變更大小調整原則，您可以變更虛擬機器記憶體或 CPU。

因應措施：無。

- **新增** NFS 停機時間會導致 VMware Cloud Director 應用裝置叢集功能無法正常運作

如果 NFS 因 NFS 共用已滿、變為唯讀等而無法使用，則會導致應用裝置叢集功能無法正常運作。當 NFS 已關閉或無法連線時，HTML5 使用者介面沒有回應。其他可能受到影響的功能包括隔離掉出現故障的主要儲存格、轉換、升階待命儲存格等。如需有關正確設定 NFS 共用儲存區的詳細資訊，請參閱 [〈準備 VMware Cloud Director 應用裝置的傳輸伺服器儲存區〉](#)。

因應措施：

- 修正 NFS 狀態，使其不為唯讀。
- 如果 NFS 共用已滿，則執行清理。

- **新增** 在多站台環境中新增 vCenter Server 和 NSX 資源時信任端點，不會將端點新增至集中式憑證儲存區域

在多站台環境中，當您使用 HTML5 使用者介面時，如果已登入 vCloud Director 10.0 站台或嘗試向 vCloud Director 10.0 站台登錄 vCenter Server 執行個體，則 VMware Cloud Director 不會將端點新增至集中式憑證儲存區域。

因應措施：

- 使用 API 將憑證匯入至 VMware Cloud Director 10.1 站台。
- 若要觸發憑證管理功能，請導覽至 VMware Cloud Director 10.1 站台的 SP 管理入口網站，移至服務的編輯對話方塊，然後按一下儲存。

- **新增 嘗試加密 vCenter Server 6.5 或更早版本中的具名磁碟失敗，並顯示錯誤**

對於 vCenter Server 執行個體版本 6.5 或更早版本，如果您嘗試將新的或現有的具名磁碟與已啟用加密的原則建立關聯，則作業失敗並顯示此版本的 vCenter Server 不支援具名磁碟加密錯誤。

因應措施：無。

- **新增 在具有 VMware Cloud Director 10.0 和 10.1 版的多站台混合環境中，信任 vCenter Server 和 NSX 連線的憑證僅適用於本機站台中的物件**

如果多站台環境中的 VMware Cloud Director 10.0 和 10.1 版互相關聯，則當您登入其中一個站台時，將無法在其他站台上登錄 vCenter Server 或 NSX Manager 執行個體。

因應措施：登入您想要在其中登錄 vCenter Server 或 NSX Manager 執行個體的站台，然後啟動登錄程序。

- **新增 在 VMware Cloud Director 租用戶入口網站中，無法從 [應用程式] 索引標籤下虛擬機器的 [進階篩選] 選項中，依資料中心篩選虛擬機器**

在 VMware Cloud Director 租用戶入口網站中，當您導覽至頂部導覽列中 [應用程式] 索引標籤下的虛擬機器時，從 [進階篩選] 選項依資料中心篩選虛擬機器會導致發生錯誤錯誤的要求：未知的內容名稱 vdcName。

因應措施：從頂部導覽列中，選取資料中心，然後選取某個資料中心以檢視其中的虛擬機器。

- **新增 延伸服務無法處理來自 VMware Cloud Director 的 RabbitMQ 訊息**

依賴 RabbitMQ 的延伸服務無法從訊息取得標頭 notification.type，因為標頭具有新的暫時名稱。VMware Cloud Director 10.1.0 的標頭名稱為 notification.operationType。

因應措施：如果延伸服務處理來自 VMware Cloud Director 的 RabbitMQ 訊息，並使用 notification.type 訊息標頭，您必須加以變更。如果 notification.type 標頭不可用，則延伸服務必須從 notification.operationType 標頭取得值。僅 10.1.0 版需要此變更。

- **在 VMware Cloud Director 服務提供者管理入口網站中，刪除組織虛擬資料中心會失敗並顯示錯誤**

在 VMware Cloud Director 服務提供者管理入口網站中，如果您將 Edge 閘道新增至組織 VDC 並啟用此閘道以提供 VMware Cloud Director 分散式路由，則嘗試以遞迴方式刪除組織 VDC 會失敗，並顯示無法刪除組織 VDC 網路錯誤訊息。

因應措施：

1. 透過使用 API，刪除組織 VDC 網路和與組織 VDC 相關聯的 Edge 閘道。
2. 透過使用 API，刪除組織 VDC。

- **如果停用提供者對舊版 API 登入端點的存取權，則依賴於系統管理員登入的所有 API 整合將停止運作，包括 vCloud Usage Meter 和 vCloud Availability for VMware Cloud Director**

從 vCloud Director 10.0 開始，您可以使用單獨的 VMware Cloud Director OpenAPI 登入端點，以供服務提供者和承租人存取 VMware Cloud Director。如果停用服務提供者對舊版 /api/sessions 端點

的存取權，則會導致與 VMware Cloud Director 整合的產品 (例如 vCloud Usage Meter 和 vCloud Availability for VMware Cloud Director) 停止運作。這些產品將需要修補程式才能繼續運作。

此問題僅影響系統管理員。承租人登入不會受到影響。

因應措施：透過使用儲存格管理工具，重新啟用服務提供者對舊版 /api/sessions 端點的存取權。

- **當您變更 VDC 的保留保證值時，即使在重新開機後，也不會相應地更新現有虛擬機器**

如果您具有使用系統預設原則的彈性組織 VDC，並且該 VDC 上已開啟電源的虛擬機器使用預設大小調整原則，則當您增加 VDC 的資源保證值時，不會更新現有虛擬機器的資源保留，並且也不會將其標記為不符合標準。當您將舊版 VDC 配置模型轉換為彈性配置模型，且現有虛擬機器在轉換後不符合彈性組織 VDC 的新預設原則時，也會發生此問題。

因應措施：

1. 若要找到虛擬機器識別碼，請在 VMware Cloud Director 租用戶入口網站中，導覽至虛擬機器的 [詳細資料] 頁面。URL 將顯示識別碼
`https://Cloud_Director_IP_address_or_host_name/tenant/.../vm-Identifier/general`
2. 若要在 VMware Cloud Director 使用者介面中顯示不符合標準的虛擬機器，請使用 VMware Cloud Director API 對虛擬機器執行明確符合性檢查。
POST: `https://VCD_IP_Address/api/vApp/vm-Identifier/action/checkComputePolicyCompliance`
3. 若要重新套用原則並重新設定資源保留，請在 VMware Cloud Director 租用戶入口網站中，針對不符合標準的虛擬機器按一下**使虛擬機器符合標準**。

- **VMware Cloud Director 顯示有關專用 vCenter Server 執行個體中的執行中虛擬機器數目、虛擬機器總計、CPU 和記憶體統計資料的錯誤資訊**

如果專用 vCenter Server 執行個體為版本 6.0 Update 3i 或更早版本、6.5 Update 2 或更早版本或者 6.7 Update 1 或更早版本，則 VMware Cloud Director 會顯示有關 vCenter Server 執行個體中的執行中虛擬機器數目、虛擬機器總計以及 CPU 和記憶體統計資訊的錯誤資訊。租用戶入口網站中的專用 vCenter Server 動態磚以及服務提供者管理入口網站中的專用 vCenter Server 資訊顯示執行中虛擬機器數目和虛擬機器總計為零，即使 vSphere 環境中有虛擬機器也是如此。

因應措施：將 vCenter Server 執行個體升級至版本 6.0 Update 3j、6.5 Update 3、6.7 Update 2 或更新版本。

- **變更已開啟電源的虛擬機器的運算原則可能會失敗**

嘗試變更已開啟電源的虛擬機器的運算原則時，如果新運算原則與具有虛擬機器群組或邏輯虛擬機器群組的提供者 VDC 運算原則相關聯，將會發生錯誤。錯誤訊息包含：基礎系統錯誤：

`com.vmware.vim.binding.vim.fault.VmHostAffinityRuleViolation。`

因應措施：關閉虛擬機器電源，然後重試該作業。

- **在 Firefox 中使用 VMware Cloud Director 服務提供者管理入口網站時，無法載入承租人網路畫面**

如果要在 Firefox 中使用 VMware Cloud Director 服務提供者管理入口網站，承租人網路畫面 (例如，組織虛擬資料中心的管理防火牆畫面) 可能無法載入。如果您的 Firefox 瀏覽器設定為封鎖第三方 Cookie，則會發生此問題。

因應措施：設定您的 Firefox 瀏覽器以允許第三方 Cookie。

- **VMware Cloud Director 10.1 僅支援 vRealize Orchestrator 工作流程的輸入參數清單**

VMware Cloud Director 10.1 支援 vRealize Orchestrator 工作流程的下列輸入參數：

- boolean
- sdkObject
- secureString
- number
- mimeAttachment
- properties
- date
- composite
- regex
- encryptedString
- array

因應措施：無

- **在啟用 VMware vSphere Storage APIs Array Integration (VAAI) 之 NFS 陣列上建立的快速佈建虛擬機器或 vSphere Virtual Volumes (VVol) 無法合併**

使用原生快照時，不支援就地合併快速佈建的虛擬機器。原生快照始終由已啟用 VAAI 的資料存放區以及 VVol 使用。當快速佈建的虛擬機器部署至其中一個儲存區容器時，無法合併該虛擬機器。

因應措施：請不要為使用已啟用 VAAI 之 NFS 或 VVol 的組織 VDC 啟用快速佈建。若要在 VAAI 或 VVol 資料存放區上合併具有快照的虛擬機器，請將虛擬機器重新放置到其他儲存區容器。

- **使用 VMware Cloud Director API 從範本建立虛擬機器且未指定預設儲存區原則時，如果沒有為範本設定預設儲存區原則，則新建立的虛擬機器會嘗試使用來源範本本身的儲存區原則**

使用 VMware Cloud Director API 從範本建立虛擬機器且未指定預設儲存區原則時，如果沒有為範本設定預設儲存區原則，則新建立的虛擬機器會嘗試使用來源範本本身的儲存區原則，而非使用您要在其中部署該範本之組織 VDC 的儲存區原則。

因應措施：無。