

# IBM Cloud Satellite 入門

2020



## 目錄

必要條件.....	3
步驟 1：建立您的位置 .....	4
步驟 2：將計算主機連接至您的位置 .....	4
步驟 3：指派您的主機至 Satellite 控制面板 .....	5
附錄一 .....	7
主機系統需求.....	7
主機儲存體與連接的裝置 .....	8
主機網路.....	8
入埠連線功能.....	9
出埠連線功能.....	9

您可以將在內部部署資料中心、其他雲端供應商或邊緣網路內的自有計算基礎架構作為「Satellite 位置」，並連接至 IBM Cloud 來建置 IBM Cloud Satellite。接著，您就可以利用 Satellite 功能在此基礎架構上執行 IBM Cloud 服務，並一致地部署、管理並管控您的應用程式工作負載。



**測試版：**IBM Cloud Satellite 有提供封閉型測試版並隨時可能變更。若要登錄此測試版，請參閱[產品詳細資料頁面](#)。

在此一入門指導教學，您將建立用於示範用途的第一個 IBM Cloud Satellite 位置。接著，您將從自己的基礎架構環境，以至少 3 個計算主機建立位置控制面板。這些計算主機可位於一個內部部署資料中心、位於 IBM Cloud 或者其他雲端供應商處。

## 必要條件

1. 您必須在自己的基礎架構環境中擁有至少 3 個符合特定要求的計算主機（例如 RHEL 7 套件）且可登入主機機器並執行 Script。
  - 所有主機必須符合[最低硬體需求](#)《附錄一》。
  - 依據雲端供應商不同，您的主機可能也需符合供應商的[特定需求](#)。
  - 針對示範用途，位置控制面板需要至少 3 個主機。



**重要事項：**一個示範用途的位置只能執行數個資源，例如一個或兩個小叢集。若您想繼續使用該位置，則需以 3 的倍數增加更多主機至該位置，例如 6、9 或 12 個主機。

若您的主機無法符合這些主機及雲端供應商需求，您就無法將主機連接至 IBM Cloud Satellite。Satellite 測試版需求仍可能變更。

2. 您必須是 IBM Cloud 帳戶擁有者，或者擁有 IBM Cloud Identity and Access Management (IAM) 中所要求的 IBM Cloud 服務的[管理者權限](#)。

## 步驟 1：建立您的位置

若要使用 Satellite，您必須建立一個位置。一個位置代表一個資料中心，您之後可增加自己的基礎架構資源，以執行 IBM Cloud 服務或其他工作負載在您自己的基礎架構上。

1. 從 [Satellite 位置儀表板](#)，按一下 **建立位置**。
2. 為您的位置輸入名稱和選擇性的說明。
3. 選取您想用來管理位置的 IBM Cloud 多可用區資料中心。如需了解為何必須選取 IBM Cloud 多可用區資料中心，請參閱 [了解 Satellite 中所支援的 IBM Cloud 多可用區資料中心](#)。確定您所選取的資料中心最靠近您計劃新增至 Satellite 位置的主機實際所在地，以確保減少 Satellite 位置及 IBM Cloud 之間的網路延遲。
4. 按一下 **建立位置**。當您建立位置時，位置相關的主要配置會被部署至位於您所選取的 IBM Cloud 多可用區資料中心中的其中一個區域上。

## 步驟 2：將計算主機連接至您的位置

透過您的位置設定程式，您現在可以將主機連接至您的位置。所有主機均必須符合 [最低硬體需求](#) 以及針對 Satellite 的任何供應商 [特定的需求](#)，且需實體位於您的內部部署資料中心，或者位於其他雲端供應商或邊緣網路。

1. 從 **主機** 標籤，按一下 **連接主機**。
2. 選用項目：可輸入任何想新增至主機的標籤，如此之後就可更易於識別主機。標籤必須以鍵值配對提供。例如，您可使用 `use:satcp` 以表示您想針對 Satellite 控制面板使用這些主機。
3. 為您的 Script 輸入檔名，或使用為您所產生的名稱。
4. 按 **下載 Script** 以產生主機 Script，並下載 Script 至您的本端機器。

**附註：**依據主機供應商不同，您可能需要在您的主機上更新所需的 RHEL 7 套件，之後方能執行 Script。例如，請參閱 [AWS](#)、[GCP](#)、[Azure](#) 或 [IBM Cloud](#) RHEL 套件更新項目。

5. 在您想連接至您位置的每個主機登入並執行 Script。依據雲端供應商不同，登入您機器的步驟亦不同。當您在機器上執行 Script 時，機器對 Satellite 位置來說是可見的，但尚未指派給 Satellite 控制面板。

a. 擷取您主機的公用 IP 位址，或者若您的主機僅有私有網路介面，則擷取您主機的私有 IP 位址。

b. 從本端機器複製 Script 至您的主機。

```
scp <path_to_script>  
root@<IP_address>:/tmp/attach.sh
```

c. 登入您的主機。

```
ssh root@<IP_address>
```

d. 執行 Script。

```
nohup bash /tmp/attach.sh &
```

6. 當您在每個機器執行 Script 時，檢查您的主機有顯示於您位置儀表板的主機標籤。當偵測到機器的活動訊號時，所有主機將顯示 **備妥** 的性能狀態，若主機尚未連接至您的 Satellite 控制面板，則將顯示狀態為 **未指派**。您必須連接至少 3 個計算主機至您的位置，如此才能繼續進行 Satellite 控制面板的設定。

### 步驟 3：指派您的主機至 Satellite 控制面板

若要完成您 Satellite 位置的設定，您必須指派 3 個在前一步驟中連接至 Satellite 控制面板的計算主機。控制面板執行元件，以安全地連接您的位置至 IBM Cloud。如需相關資訊，請參閱 [Satellite 架構](#)。

1. 從您所連接的每個主機的動作功能表中，按一下 **指派主機**。
2. 選取 **控制面板** 作為您的叢集，並選擇其中一個可用的區域。確定您將每個主機指派至不同的區域，如此您將所有 3 個主機展開至美國東部的所有 3 個區域 (**us-east-1**、**us-east-2** 和 **us-east-3**)。當您指派主機至控制面板時，IBM 會引導您的機器。此過程可能需要


數分鐘才能完成。在引導過程中，機器的性能狀態將從 **備妥** 轉變為 **配置中**。

3. 從**主機**標籤，驗證您的主機已成功地指派至 Satellite 控制面板。若指派成功時，IP 位址將新增至您的主機，而且性能狀態變更為**正常**。

**附註：**在您的主機成功地指派給控制面板後，還需要 20-30 分鐘 IBM 監控才能適當地完成您的位置設定。此外，會針對您的位置建立 DNS 記錄，且會自動登錄您主機的 IP 位址並新增至您的 DNS 記錄，以針對該位置進行負載平衡及性能檢查。此過程可能需要 30 分鐘才能完成。在此過程中，您的位置狀態將持續顯示**需要採取動作**狀態，且您可能會看到間歇性錯誤出現，例如 **Satellite 正試圖回復**或**驗證 Satellite 位置有該位置控制面板負載平衡所需的 DNS 記錄**。

# 附錄一

檢閱以下針對 IBM Cloud™ Satellite 的主機需求。有關供應商特定需求，請參閱 [供應商需求](#)。

 **附註：**無法符合這些主機需求？[聯絡 IBM 支援中心](#)並附上以下資訊：您所需的主機系統配置，您需要系統配置的原因，以及您所要建立的主機數目。

## 主機系統需求

- 主機必須在 x86 架構上執行 Red Hat Enterprise Linux 7。其他作業系統（例如 Windows）及大型主機系統（例如 IBM Z 或 Power）不受支援。
- 主機可以是實體機器或虛擬機器。
- 主機必須至少具有 4 vCPU、16 GB 記憶體和 100 GB 連接儲存體裝置。
- 主機不可含有任何額外套件、配置或其他客製項目。
- 若您的主機有 GPU 計算，請確保您安裝了節點功能探索和 NVIDIA GPU 操作器。如需相關資訊，請參閱在 [GPU 機器上部署應用程式](#)的必要條件。
- 主機必須能存取 Red Hat 更新以及下列套件。您可能需要在主機上重新整理套件。例如，在 IBM Cloud 基礎架構虛擬伺服器實例上，您可以執行 `subscription-manager refresh` 然後再執行 `subscription-manager repos --enable=*` 。

已針對此系統啟用儲存庫 'rhel-ha-for-rhel-7-server-eus-rpms'。

已針對此系統啟用儲存庫 'rhel-server-rhsc1-7-rpms'。

已針對此系統啟用儲存庫 'rhel-7-server-optional-rpms'。

已針對此系統啟用儲存庫 'rhel-7-server-eus-optional-rpms'。

已針對此系統啟用儲存庫 'rhel-7-server-rh-common-rpms'。

已針對此系統啟用儲存庫 'rhel-7-server-eus-rpms'。

已針對此系統啟用儲存庫 'rhel-ha-for-rhel-7-server-rpms'。

已針對此系統啟用儲存庫 'rhel-rs-for-rhel-7-server-eus-rpms'。

已針對此系統啟用儲存庫 'rhel-rs-for-rhel-7-server-rpms'。

已針對此系統啟用儲存庫 'rhel-7-server-rpms'。

已針對此系統啟用儲存庫 'rhel-7-server-supplementary-rpms'。

已針對此系統啟用儲存庫 'rhel-7-server-extras-rpms'。

已針對此系統啟用儲存庫 'rhel-7-server-eus-supplementary-rpms'。

- 將主機成功指派至 Satellite 位置控制面板或叢集之後，基於安全的理由，Satellite 將停用 SSH 至主機的能力。若您將主機從位置中移除或移除整個位置，您必須在主機基礎架構中重新載入機器至 SSH。否則，當您嘗試登入時，您可能會見到類似下列錯誤訊息。

許可權遭拒，請重試。

## 主機儲存體與連接的裝置

- 主機無法具有裝載至 `/var/data` 的裝置。
- 若要設定 LUKS 加密，您的主機必須具備兩個連接的磁碟：一個裝載至 `/` 的主要開機磁碟，以及一個未裝載的次要磁碟。

## 主機網路

- 請勿在您的主機上設定任何客製網路配置，例如網路管理程式 `Script`、`dnsmasq` 設定、客製 `IPTable` 規則或客製 `MTU` 設定（例如巨型頁框）。
- 所有主機必需具有相同的 `MTU` 值。
- `localhost` 值必須解析為有效的本端主機 IP 位址，通常為 `127.0.0.1`。
- 主機必須具有主機之間所有埠適用的 `TCP/UDP/ICMP Layer 3` 連線功能。封鎖特定埠可能造成不同主機間通訊封鎖，因此您不可進行封鎖。
- 您不可以使用客製的 `IPTables` 以將傳輸路線設至公用網路或私有網路，因為預設 `Satellite` 和 `Calico` 原則會置換客製的 `IPTables`。
- 下列 IP 位址範圍已保留，且無法用於您想在 `IBM Cloud Satellite` 內使用的任何網路，包括主機網路。

`172.16.0.0/16`、`172.18.0.0/16`、  
`172.19.0.0/16` 和 `172.20.0.0/16`

- 所有主機必需具有相同的預設閘道。
- 主機可以具有多個 `IPv4` 網路介面。然而，每一個主機必須具備完整的 `IPV4` 後端連線功能連至位置中的其他主機，透過網路介面連結作為預設路徑。若要尋找主機的預設網路介面，SSH 至主機並執行下列指令：

```
ip route | grep default | awk '{print $5}'
```

在此範例輸出中，`eth0` 是預設網路介面：

```
default via 161.202.250.1 dev eth0 onlink
```



## 入埠連線功能

主機必須具有透過預設閘道防火牆或系統防火牆的主要網路介面入埠連線功能。

例如，若主機的主要網路介面是 `eth0`，您必須在 `eth0` 私有網路上的預設閘道或防火牆開啟以下所需的 IP 位址。

說明	來源 IP	目的地 IP	通訊協定和埠
可讓指派給您位置服務中的主機與 Satellite 控制面板進行通訊	所有非控制面板主機	控制面板主機	TCP、UDP 30000 - 32767
存取 API 以在 OpenShift 叢集內進行變更，並透過 OpenShift 路由器存取 OpenShift Web 主控台	用戶端或授權使用者	控制面板主機	TCP 30000 - 32767
透過 OpenShift 路由器存取 OpenShift 叢集的 Web 主控台	用戶端或授權使用者	OpenShift 叢集主機	TCP 443

\*需要主要網路介面上主機的入埠連線功能

## 出埠連線功能

主機必須具有透過系統預設閘道，連至主要網路介面所有埠和 IP 位址的出埠連線功能。

例如，若主要網路介面為公用，您可嘗試使用這些指令來測試您的主機在公用網路上具有出埠連線功能。

```
ping 8.8.8.8
nslookup google.com
nslookup google.com 8.8.8.8
curl https://google.com
curl https://containers.cloud.ibm.com/v1/healthz
curl https://us.icr.io
curl -k [node 1-n]:22
```

若您不開啟所有出埠連線功能，則必須在防火牆內允許下列出埠連線功能。根據您管理 Satellite 位置的 IBM Cloud 多區域不同，所需的 IP 位址亦隨之不同。

➤ 華盛頓州特區 (wdc)

說明	來源 IP	目的地 IP	通訊協定和埠
允許控制面板工作者節點與控制面板主機通訊	控制面板主機	169.63.123.154 169.60.123.162 52.117.93.26	TCP 443、30000 - 32767 UDP 30000 - 32767
說明	來源 IP	目的地 IP	通訊協定和埠
允許主機連接至位置並指派給位置中的服務	所有主機	<a href="#">IBM Cloud 防火牆文件上 Red Hat OpenShift 步驟 2 中, 表格內美國東部列內的所有 IP 位址</a> , 或者允許所有出埠	TCP 443
允許 <a href="#">IBM Cloud 服務</a> 設定並管理您的位置	所有主機和用戶端或授權使用者	<a href="#">IBM Cloud 防火牆文件上 Red Hat OpenShift</a> 的步驟 3 - 5 中, 美國東部 (wdc) 所列出的所有 IP 位址	請參閱說明文件
允許 Satellite 配置的 Cloudflare Proxied 負載平衡器	控制面板主機	<a href="#">Cloudflare IPv4 IP</a>	TCP 443
允許 Satellite Link API 的 Cloudflare Proxied 負載平衡器	控制面板主機	<a href="#">Cloudflare IPv4 IP</a>	TCP 80、443
允許存取 Red Hat 網路時間通訊協定 (NTP) 伺服器	所有主機	0.rhel.pool.ntp.org 1.rhel.pool.ntp.org 2.rhel.pool.ntp.org 3.rhel.pool.ntp.org	

\*需要主要網路介面上主機的出埠連線功能

➤ 倫敦 (lon)

說明	來源 IP	目的地 IP	通訊協定和埠
允許控制面板工作者節點與控制面板主機通訊	控制面板主機	158.175.120.210 141.125.97.106 158.176.139.66	TCP 443、30000 - 32767 UDP 30000 - 32767

說明	來源 IP	目的地 IP	通訊協定和埠
允許主機連接至位置並指派給位置中的服務	所有主機	<a href="#">IBM Cloud 防火牆文件</a> <a href="#">上 Red Hat OpenShift 步驟 2 中，表格內英國南部列內的所有 IP 位址</a> ，或者允許所有出埠	TCP 443
允許 <a href="#">IBM Cloud 服務</a> 設定並管理您的位置	所有主機和用戶端或授權使用者	<a href="#">IBM Cloud 防火牆文件</a> <a href="#">上 Red Hat OpenShift 的步驟 3 - 5 中，英國南部 (lon) 所列出的所有 IP 位址</a>	請參閱說明文件
允許 <a href="#">Satellite 配置</a> 的 <a href="#">Cloudflare Proxied 負載平衡器</a>	控制面板主機	<a href="#">Cloudflare IPv4 IP</a>	TCP 443
允許 <a href="#">Satellite Link API</a> 的 <a href="#">Cloudflare Proxied 負載平衡器</a>	控制面板主機	<a href="#">Cloudflare IPv4 IP</a>	TCP 80、443
允許存取 <a href="#">Red Hat 網路時間通訊協定 (NTP) 伺服器</a>	所有主機	0.rhel.pool.ntp.org 1.rhel.pool.ntp.org 2.rhel.pool.ntp.org 3.rhel.pool.ntp.org	-

\*需要主要網路介面上主機的出埠連線功能

© Copyright IBM Corporation 2020.

IBM、IBM 標誌和 [ibm.com](#) 是 International Business Machines Corp. 在全世界許多司法管轄區註冊的商標。其他產品與服務名稱可能是 IBM 或其他公司的商標。IBM 商標最新清單可於下列網站之「著作權與商標資訊」(Copyright and trademark information) 網頁上取得：[www.ibm.com/legal/copytrade.shtml](#)。

本文件從初始發佈日期開始保持最新，IBM 得隨時變更。並非所有產品與服務都會在 IBM 營運的每個國家或地區供應。文中引用的效能資料和客戶範例僅供示意用途。實際效能結果可能會視特定配置與作業條件而異。本文件中的資訊係「依現狀」提供，不含任何明示或默示之保證，也不含適售性、特定目的之適用性及無侵權之保證。IBM 產品依相關合約條款之規定提供保證。良好安全作法聲明：IT 系統安全涉及透過預防、偵測與回應您企業內外部不當存取來保護系統和資訊安全。不當存取可能導致資訊遭到更改、破壞、不當使用或濫用，或者造成毀損或濫用您的系統，包括用來攻擊其他對象。沒有任何 IT 系統或產品是絕對安全，也不可能有任何產品、服務或安全措施有辦法完全杜絕不當使用或存取。IBM 系統、產品及服務的設計理念是相互組合成一種符合法規的綜合性安全方法，其中必然涉及其他作業程序，另外可能需要運用其他的系統、產品或服務才能發揮最大效用。IBM 不保證任何系統、產品或服務免於或將使您的企業免於任一方的惡意或非法行為。