

## IBM QRadar on Cloud

本「服務說明」說明本「雲端服務」。適用之訂購文件提供「客戶」訂單有關計價及其他詳細資料。

### 1. 雲端服務

#### 1.1 IBM QRadar on Cloud

「客戶」得從下列可用供應項目選取其所要供應項目。

##### 1.1.1 IBM QRadar on Cloud 100 EPS

IBM QRadar on Cloud 供應項目藉由以 IBM Security QRadar SIEM 產品為基礎之 IBM Cloud，提供進階安全情報解決方案。此供應項目可讓「客戶」蒐集、產生關聯及儲存從就地部署及雲端環境產生之事件，以及執行安全與威脅管理，執行方式同於就地部署之 QRadar SIEM 產品。此外，在本供應項目中，IBM 還提供一天 24 小時之基礎架構監視，並於有可用之最新軟體層級或重要修補程式時予以套用。

本項「雲端服務」包含九十天有效之可供搜尋的儲存體。

#### 1.2 選用服務

##### 1.2.1 IBM QRadar on Cloud 1K EPS Temporary Upgrade

一種服務升級，可提供用於蒐集及處理日誌事件之額外 1000 EPS 容量，惟僅適用於暫時性之數個月。

「客戶」可購買多個單位之本升級，惟以本供應項目可支援之最高 EPS 層級為上限。其目的在於透過暫時性容量升級，符合特定「客戶」一年中偶爾需要應付突增使用量之需求。於前項期間結束時，將從「客戶」之環境移除該等暫時性容量增加數量。

##### 1.2.2 IBM QRadar on Cloud Data Storage 100 EPS

資料儲存容量升級可新增額外儲存體及擴充分析期間。容量升級，就所購買之各 100 EPS 升級項目，最多上限可提供「客戶」一整年之資料儲存。

##### 1.2.3 IBM QRadar on Cloud Flows Add-On

與 IBM QRadar SIEM 及流程處理器整合，以提供第 3 層網路可見度及流程分析，進而協助「客戶」對其整個網路中之各項活動進行感應、偵測及回應。

##### 1.2.4 IBM QRadar on Cloud Vulnerability Management Add-On

主動感應及探索網路裝置及應用程式安全漏洞、新增環境定義，以及支援安全漏洞修正及調整動作之優先順序。

##### 1.2.5 IBM QRadar on Cloud Log Archival

容許「客戶」保存「雲端服務」在訂用期間內之事件資料。IBM 協同「客戶」將指定事件寫至物件儲存體，作為保存之用。應「客戶」之要求，IBM 將在該要求的三個工作日內將至多長達三十天的保存事件資料重載至「客戶」的「雲端服務」實例。在返回到保存物件儲存體之前 48 小時內，該等資料仍可供「客戶」使用。「客戶」每三個月的期間得提出最多兩個要求。容量升級，就所購買之各 100 EPS 升級項目，最多上限可提供「客戶」一整年之資料儲存。

#### 1.3 Acceleration Services

##### 1.3.1 IBM QRadar on Cloud Optimization Service

對於此遠端交付之訂用服務，IBM 將與「客戶」舉行審查會議，以評估「客戶」之本項「雲端服務」實例的現行性能，及透過 QRadar on Cloud Health Status 報告交付結果予「客戶」，該報告將指出是否有任何需要改進之處。

此外，IBM 將應「客戶」之要求，在一年期間內（最多八天）提供任何下列諮詢服務予「客戶」：

- 協助新增其他日誌來源至「雲端服務」；
- 配置其他的搜尋、報告和儀表板；

- 對現有的 QRadar 部署執行其他調整；以及
- 提供對於相關 QRadar 主題之知識移轉。

### 1.3.2 設定服務

下列安裝服務由遠端交付，可個別訂購。不論是否用完所有時數（視適用情形而定），除有特別註明外，所訂購之各項服務將於購買日起九十天後到期。前述服務包含一個指定的「IBM 業務經理」，由其安排啟動會議。

### 1.3.3 IBM QRadar on Cloud Deployment Service

本項服務提供四十小時之專業服務，在此期間 IBM 將執行下列部分或全部作業：

IBM 將舉行至多持續十六小時的 SIEM 架構審查，以定義「客戶」的報告需求，並將其發現項目以一份解決方案架構報告交付予「客戶」，以協助定義及擷取「客戶」之需求。

該項報告將包括：

- 「客戶」定義之報告需求，以協助符合「客戶」之循規、審核及安全情報需求。
- IBM 得協助實作之安全情報需求、使用案例及應用程式（最多十個使用案例及最多兩個應用程式）。
- 為支援使用案例所必需有關「客戶」日誌及流程來源之高階資訊。
- 網路基礎架構考量，例如防火牆和連接埠。

如剩餘時間容許，IBM 將根據解決方案架構報告執行下列作業：

- 在「雲端服務」中配置最多十個日誌來源類型的三個實例之事件組合。該活動包括將知識移轉至「客戶」相關人員，使其得視需要新增更多日誌來源。僅標準 QRadar 裝置支援模組 (DSM) 所支援的日誌來源才會包含在本服務中。
- 起始調整包括 a) 啟動現成可用之規則、已儲存的搜尋、累計時間序列圖形及報告；b) 識別及移除雜訊來源；以及 c) 透過 NFS、CIFS 或 iSCSI 配置離線儲存體。
- 實施該解決方案架構文件所記載之 IBM QRadar App Exchange 中的十個使用案例及兩個應用程式。

### 1.3.4 IBM QRadar on Cloud Custom Parser Service

本服務將提供單一客製剖析器/uDSM 的開發，以支援要傳送至「雲端服務」之「客戶」非標準日誌來源類型，並包含下列作業：

- 建立一種非標準日誌來源類型的客製剖析器（從遠端執行的工作）；
- 建立、配置及對映 uDSM；
- 部署及測試客製 uDSM；以及
- 為日誌來源剖析至多二十五種訊息類型。

## 2. 資料處理及保護 Data Sheet

以下鏈結中之「IBM 資料處理附錄」（網址：<http://ibm.com/dpa>）(DPA) 及「資料處理及保護 Data Sheet」（稱為 Data Sheet 或「DPA 附件」）提供有關「雲端服務」之其他資料保護資訊，以及有關可能處理之「內容」類型、所涉及之處理活動、資料保護特殊功能及「內容」保留與歸還相關細節等事宜之選項。若歐盟一般資料保護規章 (EU/2016/679) (GDPR) 適用於「內容」所含個人資料，則於其適用的範圍內，適用前揭 DPA。

<https://www.ibm.com/software/reports/compatibility/clarity-reports/report/html/softwareReqsForProduct?deliverableId=FB0F42F0750011E6865BC3F213DB63F7>

## 3. 服務水準及技術支援

### 3.1 服務水準協定 (SLA)

IBM 為「客戶」提供下列可用度服務水準協定 (SLA)。IBM 將依本「雲端服務」累計可用度，套用最高可適用之補償，如下表所示。可用度百分比之計算方式如下：合約月份中的總分鐘數減去合約月份中「服務停用」之總分鐘數，除以合約月份之總分鐘數。「服務停用」定義、請求的處理及如何洽詢 IBM 有關服務

可用度問題，均載明於 IBM SaaS 支援概觀（網址：[https://www.ibm.com/software/support/saas\\_support\\_overview.html](https://www.ibm.com/software/support/saas_support_overview.html)）。

可用性	扣抵 (每月訂用費用之 %*)
小於 99.9%	2%
小於 99.0%	5%
小於 95.0%	10%

\* 訂用費用為請求時當月之約定價格。

## 3.2 技術支援

於 IBM 支援手冊（網址：<https://www.ibm.com/support/home/pages/support-guide/>）中選取本「雲端服務」，即可找到本「雲端服務」之技術支援（包括支援聯絡人詳細資料、嚴重性層次、可用支援時數、回應時間及其他支援資訊與處理程序）。

## 4. 計費

### 4.1 計費度量

本「雲端服務」之計費度量載明於「交易文件」中。

下列計費度量適用於本「雲端服務」：

- 「約定」為「雲端服務」有關專業或訓練服務。
- 「每秒事件數量」係指藉由「雲端服務」之使用而予以處理或與其相關之特定事件每秒發生次數。
- 「每分鐘流程數量」為「雲端服務」每分鐘所管理或處理之流程數量。一個「流程」係指二部主機間之一筆通訊記錄。內含相同來源 IP、目的地 IP、來源埠、目的地埠及通訊協定之封包，結合為一筆「流程」記錄。
- 「資產」係為「雲端服務」所存取或管理之具有相當價值之唯一識別有形資源或項目。

## 5. 附加條款

於 2019 年 1 月 1 日前簽署之「雲端服務合約」（或等同的基本雲端合約），適用 <https://www.ibm.com/acs> 所載明之條款。

### 5.1 啟用軟體

本「雲端服務」內含下列「啟用軟體」：

- Data Gateway - 「客戶」最多僅限安裝及使用十 (10) 份 Data Gateway。

## 6. 置換條款

### 6.1 安全資料使用

雙方當事人所訂基本「雲端服務」條款之「內容及資料保護」一節另有規定者，下列條款較該等規定優先適用：IBM 就使用於網路威脅情報之情形（具體而言，亦即 URL、IP 位址、網域及檔案雜湊），得從「客戶內容」蒐集潛在惡意活動指標。前揭指標顯示「客戶」網路威脅風險提升者，IBM 得通知「客戶」。