技術白皮書

PcVueSolutions 架構和部署

Last update :	May 2019
Revision :	7
Content :	介紹PcVue 解決方案的架構和部署
Confidentiality :	公開

PcVue Solutions

目錄

1. 概況

此文檔介紹了部署監控軟體的一些選項。
部署是將角色分配給工作站和伺服器以滿足給定實際網路架構中的系統要求的過程。
出於本主題的目的，我們將考慮監控軟體具有以下主要功能：

- **資料獲取** - 資料獲取 – 使用 Modbus，OPC 等通信協議收集即時資料，表示實際值或計算值...
- **歷史資料歸檔** – 記錄即時資料，以便以後可以由主管本身或協力廠商應用程式訪問。
- **報警** – 報警的生成和管理。
- **HMI** – 人機界面，作為展示層的圖形介面，使操作員能夠與監控系統進行交互。
- **多站** – 監控軟體在網路架構中的網站之間分配即時和歷史資料的機制。
- **Web 伺服器擴展** – 用於將監控軟體核心架構與 Web 用戶端連接的一組元件。
- **和協力廠商系統的介面** – 比如 CMMS, GIS, ERP, MES...

實現功能和角色分配依賴於授權。 有關授權的更多資訊，請聯繫當地的銷售代表。

1.1 架構

典型架構如下：

- **單機版** – 所有SCADA功能都集成在一個工作站中。

- **多站架構** – 基於客戶/伺服器架構的SCADA。

- **高可用性架構** – 分散式SCADA功能和角色，以提供更好的彈性和可擴展性。 多站部署包括以下特定方案：
  - **資料獲取複聯** – 兩個或多個站配置為複聯（熱備用）。
  - **歷史資料複聯** – 兩個或多個站配置為複聯（熱備用）。
  - **互聯伺服器**。

- **三層架構** – 使用一個或多個站作為閘道

- **工程師站** – 帶有版本管理功能。

- **Web & mobile** – Web後端伺服器以及基於Web和移動用戶端。

1.2 角色

上述架構需要分配一下角色：

- **資料獲取**
  - 與現場設備通信，
  - 即時資料和報警生產，
  - 為其他站提供即時資料和警報。
- **歷史資料**
  - 使用其他站產生的即時資料和警報，
  - 處理資料存儲，記錄和重放歷史資料，
  - 管理與 RDBMS 的連接，
  - 將歷史資料提供給其他站。
- **Web 後端伺服器**
  - 使用其他站產生的即時資料和警報，
  - 使用其他站保存的歷史資料，
  - 管理與 IIS 的介面，
  - 為 Web 用戶端提供服務，包括 WebVue 用戶端，TouchVue 用戶端，WebScheduler 和 Web Services Toolkit 用戶端
- **閘道**
  - 用於在兩個網路之間安全地傳輸資料
  - 在一個網路上消耗其他電臺產生的即時資料，警報和歷史資料，
  - 為另一個網路上的網站提供即時資料，警報和歷史資料。
- **HMI**
  - 向使用者顯示類比，圖形，報警檢視器，日誌檢視器，趨勢檢視器...

根據角色的組合，監控軟體的工作站可以更好地部署在桌面作業系統或伺服器作業系統上。

1.3 架構圖例

1.3.1 圖例


HTML5


防火牆


Web 後端伺服器


專利型歸檔單元


HDS 歸檔單元


單機站


PcVue 訪問

伺服器站


中央版本資料夾


FrontVue


PcVue 實例

用戶端站

Building blocks	Typical roles	Typical deployment mode
Standalone station 	• Data Acquisition • Historical data • HMI • Does not have the capability to exchange data with other stations	• As a Desktop Application • Under a desktop OS
SCADA station 	• Data Acquisition • Historical data • HMI	• As a Desktop Application if it requires an HMI • Under a desktop OS Or • As a Windows Service if an HMI is not required • Under a server OS
Data acquisition server 	• Data Acquisition	• As a Windows Service • Under a server OS
Client station 	• HMI	• As a Desktop Application • Under a desktop OS • Or with a server OS hosting Remote Desktop Services combined with lightweight terminals used as operator workstations
Historical data server 	• Historical data	• As a Windows Service • Under a server OS
Web server 	• Web server	• As a Windows Service • Under a server OS
Web clients 	• Remote monitoring and control over the Internet or Intranet. • WebVue clients and TouchVue clients.	• Using a Web browser or a Web App • On a desktop PC or a mobile device

Engineering station

- Depending on the architecture and project design, an engineering station can have very different roles, ranging from those of a data acquisition server (for testing communication with field devices), to archive server or just an HMI workstation (to design mimics).
- Project development and maintenance.
- Project and libraries version management.
- Interoperability with third-party generation tools.

- As a Desktop Application
- Under a desktop OS

2. 架構示例

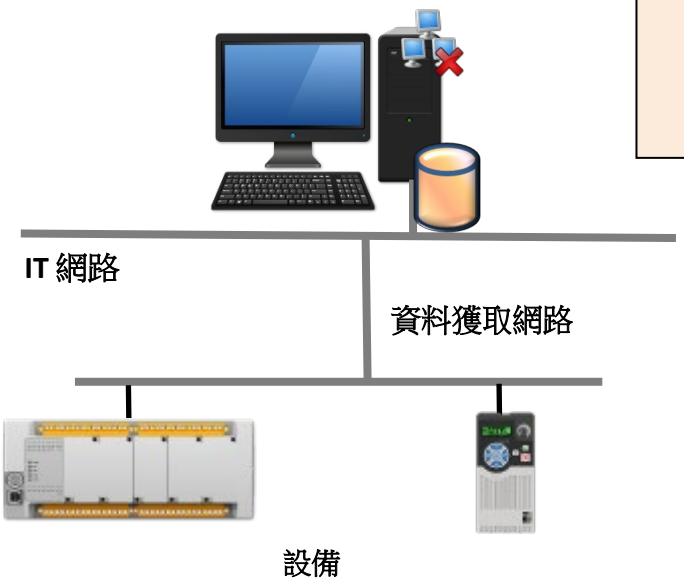
本主題描述了最常見的基本架構。根據以下因素，有許多變化可以滿足系統要求

- 用戶數量
- 操作員站的類型和數量（HMI）
- 可用性
- 靈活性
- 可擴展性
- 恢復力
- 維護和應用程式生命週期管理

請聯繫技術支援以獲取更多資訊。

2.1 單機站

- ✓ 最簡單的架構
- ✓ 全部監控集中在“一體化”的工作站上
- ✓ 單機 PcVue 站負擔所有功能



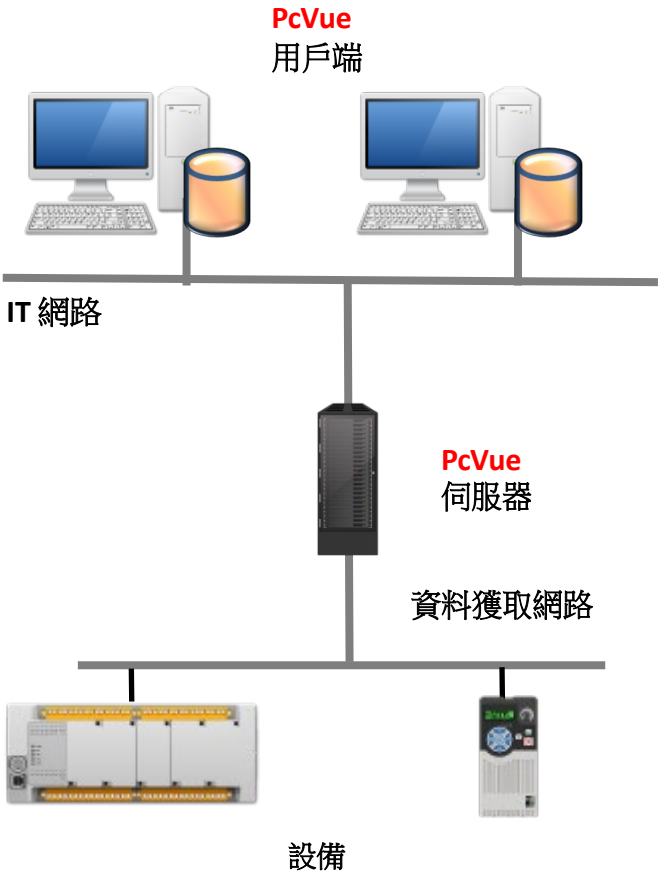
獨立站通常是操作員直接操作，它是最簡單的架構，所有功能和角色都集成在一個站中

在傳統的單使用者配置中，PcVue 監視和/或控制工業網路上的所有設備，並且還處理使用者請求。 PcVue 可以在單個站上支援數萬個變數。
PcVue 單機站是一個一體化的獨立 HMI 站，使用 PcVue 的標準功能監視和控制您的專案：

- ✓ 資料獲取，
- ✓ 即時資料庫，
- ✓ HMI，
- ✓ 歸檔，
- ✓ 警報和日誌，
- ✓ 趨勢，
- ✓ 資料處理，報表
- ✓ 用戶管理

2.2 多站

- ✓ 最簡單的多站架構
- ✓ 從幾個遠端用戶站監控項目
- ✓ 優化資料處理網路負載



最簡單的用戶端/伺服器架構，適用於需要多個使用者工作站與工業網路連接的應用程式。
伺服器是與設備通信並將資料廣播到用戶端（或消費者）站的資料來源站（生產者）。
PcVue 站之間的通信非同步工作，並使用 PcVue TCP/IP 消息傳送資料包中的資料。
伺服器站可以僅是完整的用戶操作站或資料獲取伺服器。它執行專案的所有資料處理。 歷史資料歸檔可以僅在伺服器端上實現，也可以在每個客戶站的本地實現。
用戶端可以使用任何支持 TCP/IP 並保證足夠頻寬的媒體連接到位於另一個位置的伺服器，包括撥號網路，甚至是衛星鏈路。

通常是在 2 個不同的伺服器上分別實現變數的資料獲取和歷史資料存儲，或讓用戶端在本機存放區歷史資料。

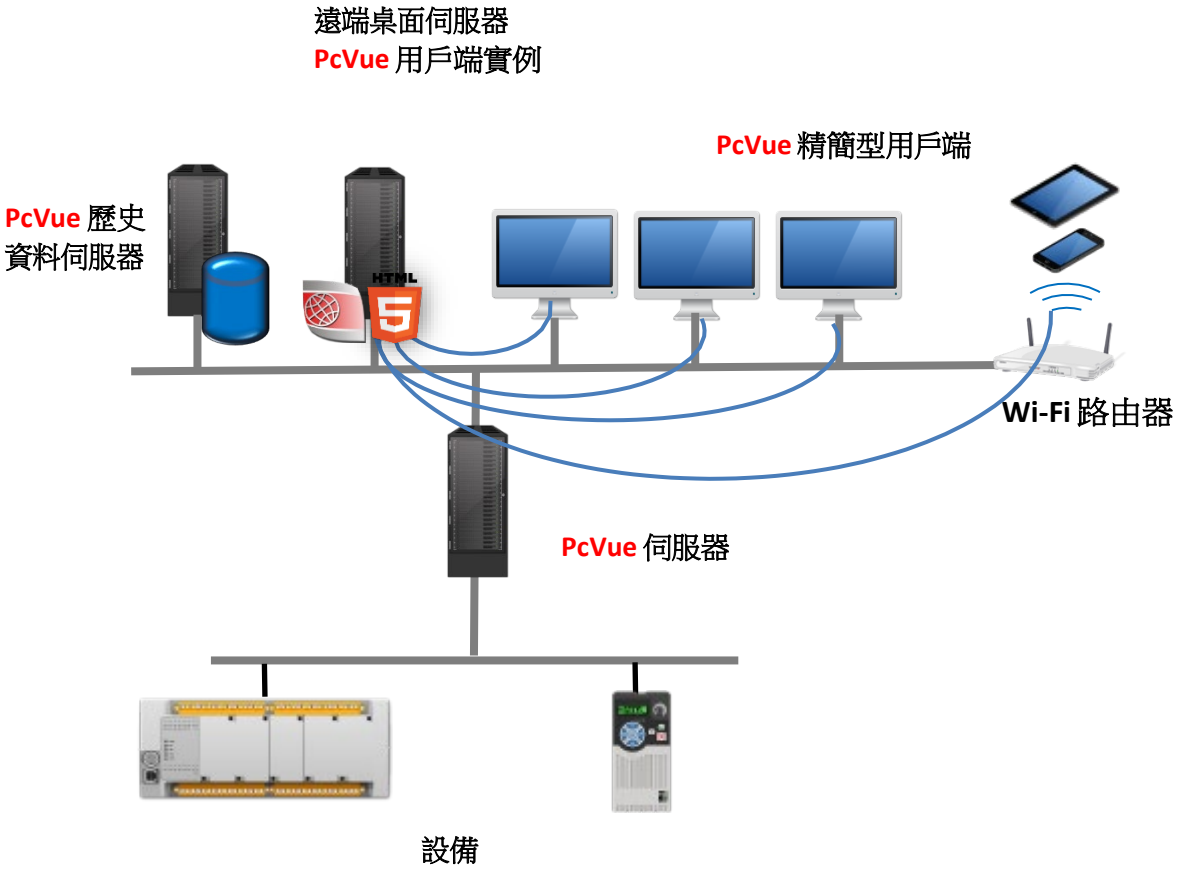
2.3 帶遠端桌面伺服器的多站-用於部署用戶端工作站

- ✓ 減少管理工作量和成本
- ✓ 低成本的瘦硬體用戶端
- ✓ 在精簡型用戶端上免費安裝

Windows Server 配置了遠端桌面服務時，允許多個使用者同時使用單個伺服器的資源並執行伺服器上安裝的應用程式。使用者通過網路連接到伺服器的精簡型用戶端（也稱為終
端）與應用程式交互。以這種方式連接到 Windows Server 的使用者的過程稱為遠端桌面會話，並使用稱為遠端桌面協定（RDP）的標準。精簡型用戶端（包括 Linux 或 Unix 下的 Wyse Thin Computing 終端）使用 RDP 用戶端軟體來管理 RDP。

除了使用遠端桌面運行會話外，Windows Server 還使用本地監視器，鍵盤和滑鼠運行會話。這稱為本地會話（或有時稱為控制台會話或互動式會話）。

在 RD 工作階段主機伺服器上運行監控軟體時，可以從每個遠端桌面會話和/或本地會話運行監控軟體的實例。僅安裝了監控軟體的一個副本。



從監控軟體的網路角度來看，這種架構與之前的架構相同，只是作為合理化部署的一種方式使用客戶站，RDS 和羽量級終端。

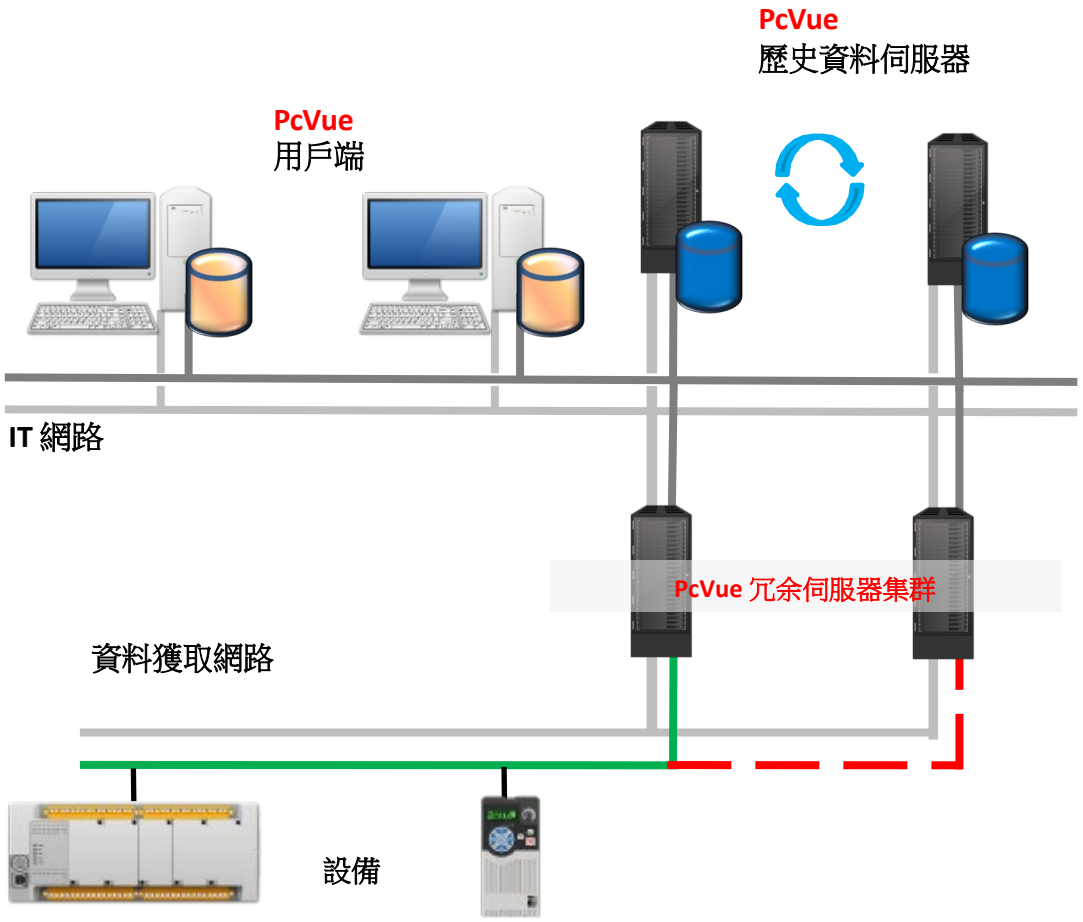
在此示例中，PcVue 用戶端安裝在 Windows Server 作為遠端桌面伺服器（RDS）運行的工作站上。

此工作站是 RD 工作階段主機伺服器並託管 PcVue 用戶端實例。用戶可以從任何精簡型用戶端打開遠端桌面會話並運行 PcVue 用戶端實例。伺服器上的 HTML5 介面允許任何配備符合 HTML5 標準的 Web 流覽器的精簡型用戶端通過 RDS 實例訪問 PcVue 應用程式。

只有一個 PcVue 伺服器也可以駐留在 RD 工作階段主機伺服器上。
必須將 RD 工作階段主機伺服器配置為承載多個用戶端實例，以支援所需數量的同時會話。精簡型用戶端不需要任何特定安裝，這有助於現場部署應用程式。

2.4 高可用性

- ✓ 非常高的安全性和系統/資料可用性
- ✓ 使用雙網路及安全的用戶端 – 伺服器設置
- ✓ 多用戶站
- ✓ 優化的資料處理和現場網路資料負載



當需要更高的可用性和彈性時，這種更加分散的體系架構可以帶來複聯和角色分離。它類似於多站架構，但具有資料獲取伺服器和歷史資料伺服器分離和複聯。

站之間可以使用雙網路（LAN 和/或 WAN），現場網路也可以使用雙網路。這樣在任何客戶站和資料來源站之間有兩條獨立的網路路徑。每個 PcVue 用戶端站與每個伺服器站之間保持兩個連接通道，並且僅當這兩個連接通道都不可用時才會嘗試進行伺服器之間的切換。

在工業乙太網網路中，PcVue 可以管理通信介質複聯和設備複聯。

每個工作站都可以歸檔資料，以提高歷史資料的可用性。

通常其他架構還包括 Web 伺服器和 Web 用戶端。

2.4.1 即時伺服器複聯

即時伺服器專用於採集 PLC 的資料並即時更新客戶站的即時資料。 用戶端站擁有圖形介面，用於監視和控制專案。
這兩台伺服器之間是複聯的，並為客戶站提供即時資料。

2.4.2 單主動採集伺服器模式

伺服器以單主動採集伺服器模式運行。與工業網路通信的伺服器稱為“主動”。另一台伺服器稱為“被動”。只有主動伺服器和 PLC 通信，為用戶端站提供即時資料並同步被動伺服器。
在主動伺服器發生故障的情況下，被動伺服器啟動其與 PLC 通信並提供資料給用戶端站。熱備切換完成並且完全無縫地與操作員進行切換。
當啟動伺服器時，有兩種可能的情況：
•其他伺服器不工作。新伺服器啟動工業網路上的通信以刷新其設備變數並成為主動伺服器。網路中的所有用戶端都會自動訂閱變數。
•另一台伺服器已在運行並處於主動狀態。新伺服器自動變為被動並與動態伺服器同步。
當被動伺服器變為主動狀態時，工業網路上的通信恢復立即生效，這使新的主動伺服器立即運行。
主動伺服器在時間 T 通過事件自動觸發客戶站。對於操作員來說，訪問資訊（控制/命令/確認/存檔...）在任何站都是相同的;無論網路狀態如何，資料來源都完全透明。
根據使用者設定檔，可以從任何用戶端工作站訪問全部或部分站資料點。
在任何網站都可以知道所有網路站的狀態和採集系統上的通信。該系統提供了一個完整的架構圖，可以即時顯示與其連接的 PLC 和組態軟體。
系統可以根據授權，對複聯狀態進行切換，實現伺服器維護。（例如：強制被動伺服器變為主動狀態）。

2.4.3 歷史伺服器複聯

2.4.3.1 帶兩個同步資料庫的模式

兩台歷史伺服器在兩個獨立的 SQLServer 關聯式資料庫上並行記錄資訊。兩台伺服器同時記錄相同的資訊。
先前可配置的日期範圍資訊將自動清除，通過這種方式控制資料庫的大小，與保存長時間的資料相比，這樣可以保證更快的存取時間。
如有必要，可以從 ASCII 檔中提取已清除的記錄以“備份”。
定期自動合併缺失的資訊以管理可能的系統停止（故障或維護）情況。這種合併是橫向完成的：第一台伺服器在第二台伺服器上提取其缺失的歷史記錄，反之亦然。在合

併結束時，關聯式資料庫是相同的。

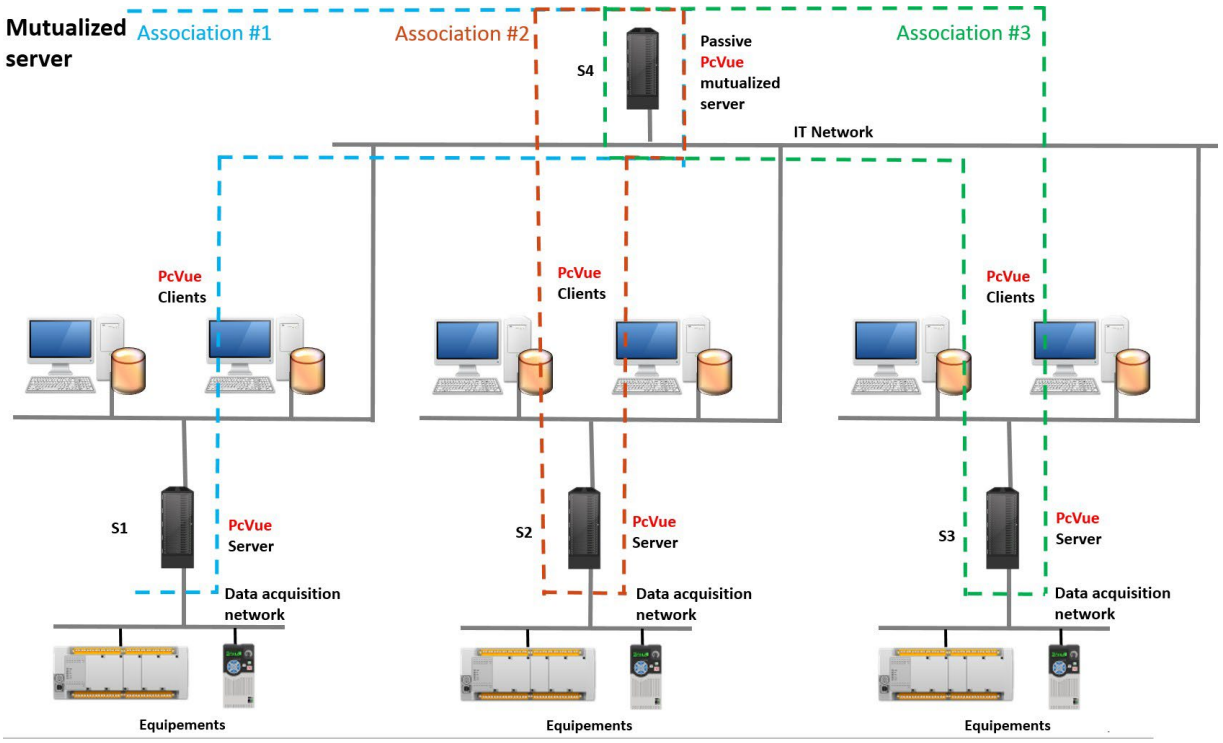
合併與標準訪問（讀取或寫入）及通訊並行運行。
每個監控軟體用戶端透明地訪問主動伺服器的歷史記錄，因此可以從任何用戶端網站查看連續存檔的資料。

2.4.3.2 帶一個資料庫的模式

原理是一台機器運行管資料庫和 SQL Server 引擎（最好是 Windows Server 作業系統），它與兩台即時伺服器 PcVue 是不一樣的。
遵循先前描述的單主動伺服器原理，只有主動的 PcVue 伺服器將資訊存儲在資料庫中。因此，在所有情況下，始終至少有一個歷史伺服器可以存檔資訊。
如果資料庫機器出現故障，則主動的 PcVue 伺服器會在本機存放區資訊。 當與 SQL Server 資料庫的連接恢復時，主動伺服器將本地生成的存檔傳輸到中央資料庫。只要有一台歷史伺服器正常運行，其集成的功能就能夠確保存檔的連續性。

2.5 多重複聯伺服器

- ✓ 優化的冗餘架構，用於監控和控制多個項目
- ✓ 減少部署和維護工作



多重複聯架構是高可用性架構的一個擴展。
當您必須監視和控制多個流程，生產線，工廠，建築物，網站..... 並且需要可靠的網路時，您可以設置一個高端伺服器，該伺服器將用作多個區域的備用伺服器。 通過共用備用伺服器，您可以實現複聯和可用性，同時最大限度地減少部署和維護完全重複伺服器集群的工作量和成本。

此架構可能不能應用在任何通訊協定中，請聯繫技術支援以獲取更多資訊。

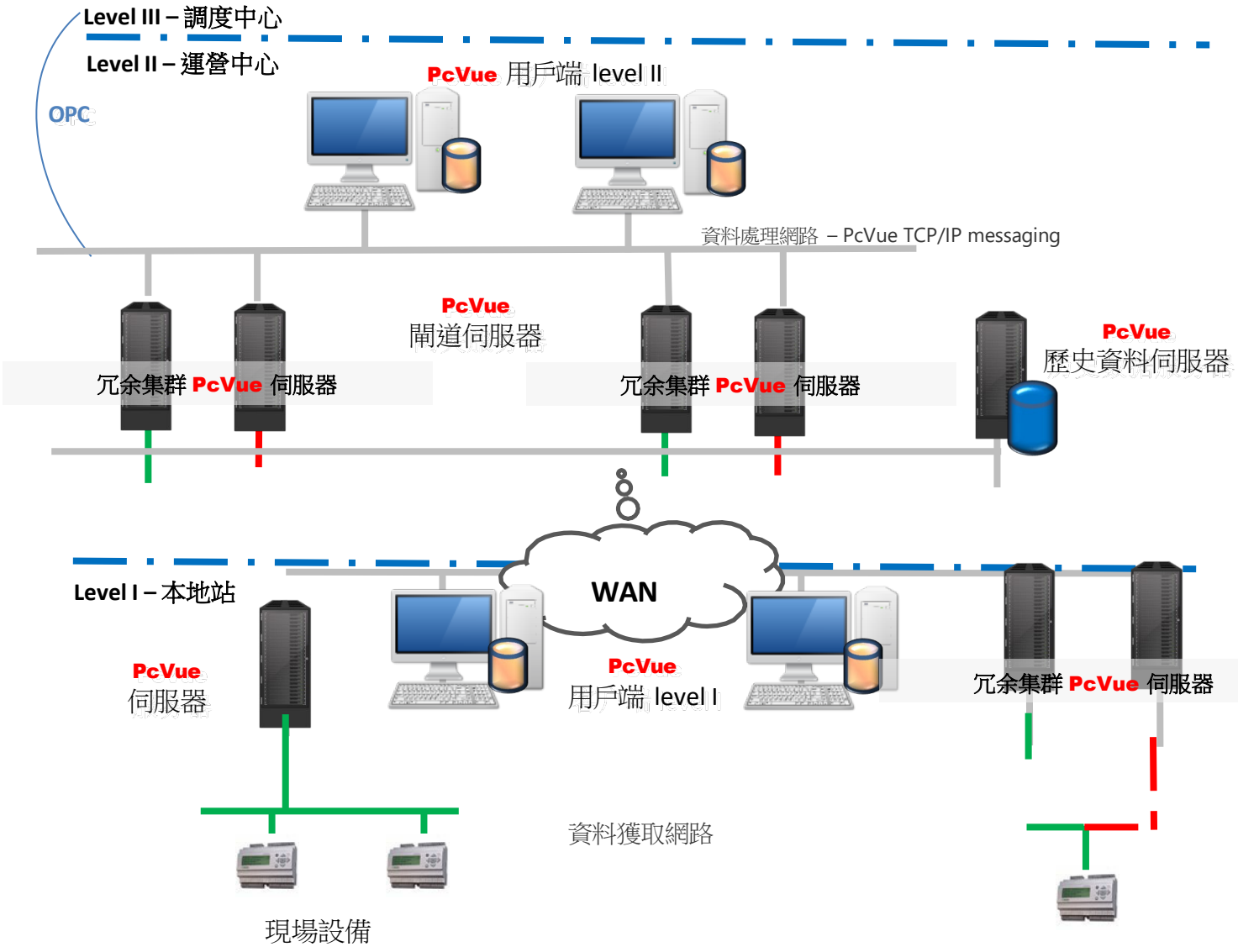
2.6 多層架構

當網路需要分段時，可以將閘道添加到架構中。
例如，當系統跨廣域網路時，或者當資料消費者站（客戶站或資料存存儲）位於不太可信的網路中時，這種架構是有用的。
這樣的閘道可以部署在DMZ中，如果需要，閘道可以是複聯的。

在分散式架構中，每個站即可以是一些變數的資料來源站（生產者），又可以是另一些變數的消費者站。此外，一些站可以充當位於另一區域的中央控制室的資料集中器。
PcVue允許開發和部署多伺服器/多用戶端應用程式，其中部分伺服器集群配置為從設備採集資料，部分伺服器集群配置為從其他伺服器採集資料（如用戶端）。
中央伺服器僅採集所有資料的子集，以便更高效地效監控設備

2.6.1 多層架構：部署#1

- ✓ 適用于超大規模應用和地理分佈廣泛的系統
- ✓ 不同級別控制
- ✓ 非常靈活



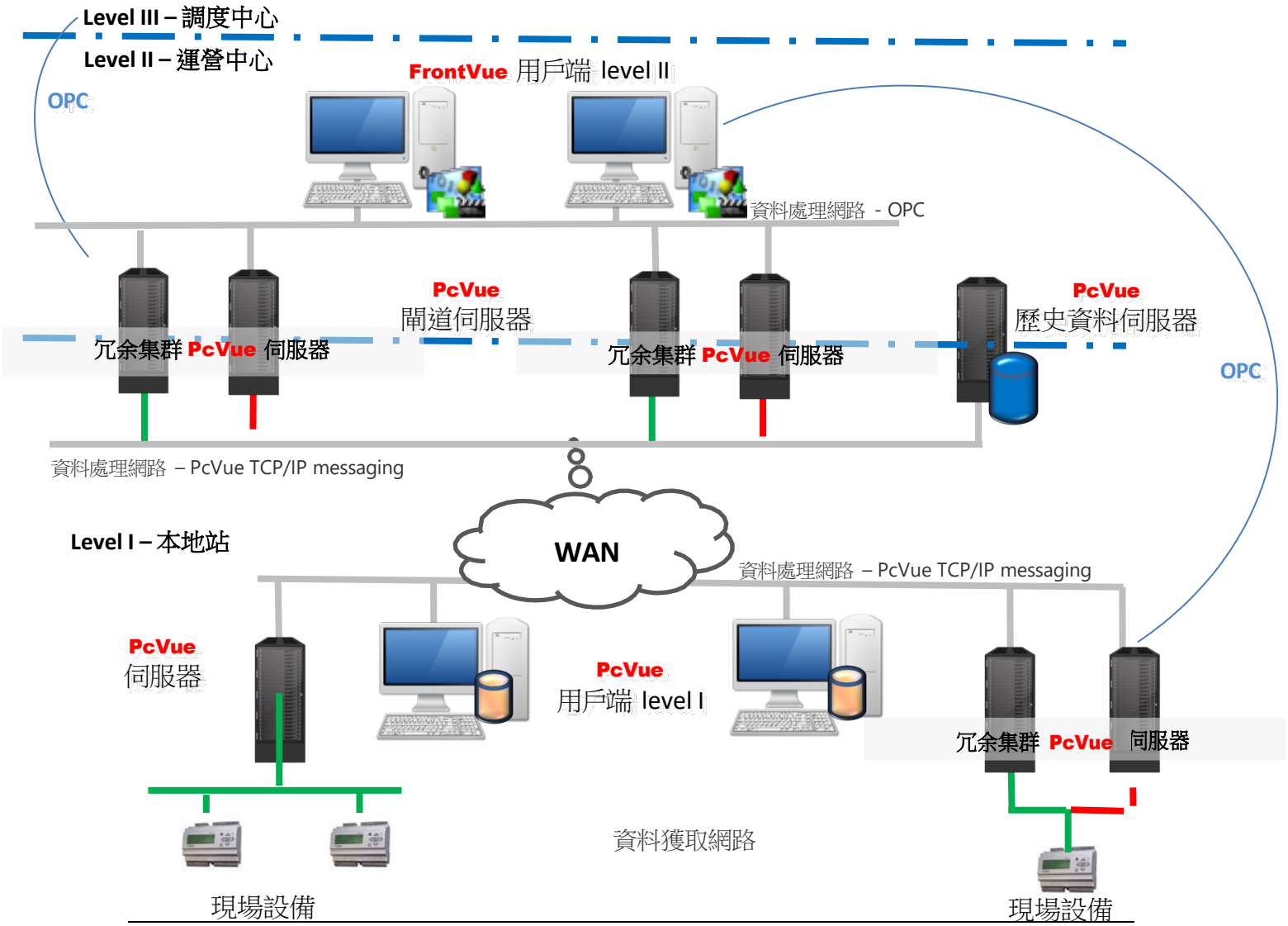
I 級 – **本地網**站由廣泛分佈的 PcVue 站組成，從現場設備獲取資料，並通過具有衛星連接的廣域網路將資料提供給 II 級。

II 級 – **操作中心**是系統架構的核心，具有 PcVue 伺服器的冗余集群，以集中來自 I 級的不同站的資料。伺服器的每個集群處理數千個即時變數並在本地歸檔更重要的變數資料。

一對伺服器也可以專用於將低級別的重要資料存檔到 DBMS。
連接到伺服器站的用戶端站用作操作和工程控制台，並說明操作員監視和控制來自任何網站的變數（即時，報警.....）。
III 級 – **調度中心**是該架構的最高級別。 它通過 OPC 從級別 II 統獲取主要資料。

2.6.2 多層架構：部署#2

- ✓ 適用於地理分佈廣泛的系統
- ✓ 多個級別的控制
- ✓ 對於非常**大量的資料**/高增長率專案
- ✓ 非常靈活



當應用程式變得更大（超過 30 萬個變數）時，使用更羽量級的 FrontVue HMI 用戶端優化系統架構、替換全功能的 PcVue 用戶端是有意義的，以確保系統的可擴展性。

FrontVue 是一個非常羽量級的基於 OPC 的 HMI 用戶端，沒有嵌入式處理或存檔。 它作為 OPC 用戶端連接到 PcVue，它可以監控和控制即時資料，並可以顯示在 PcVue 端管理的報警和歷史資料。

FrontVue僅刷新顯示的資料以便於：

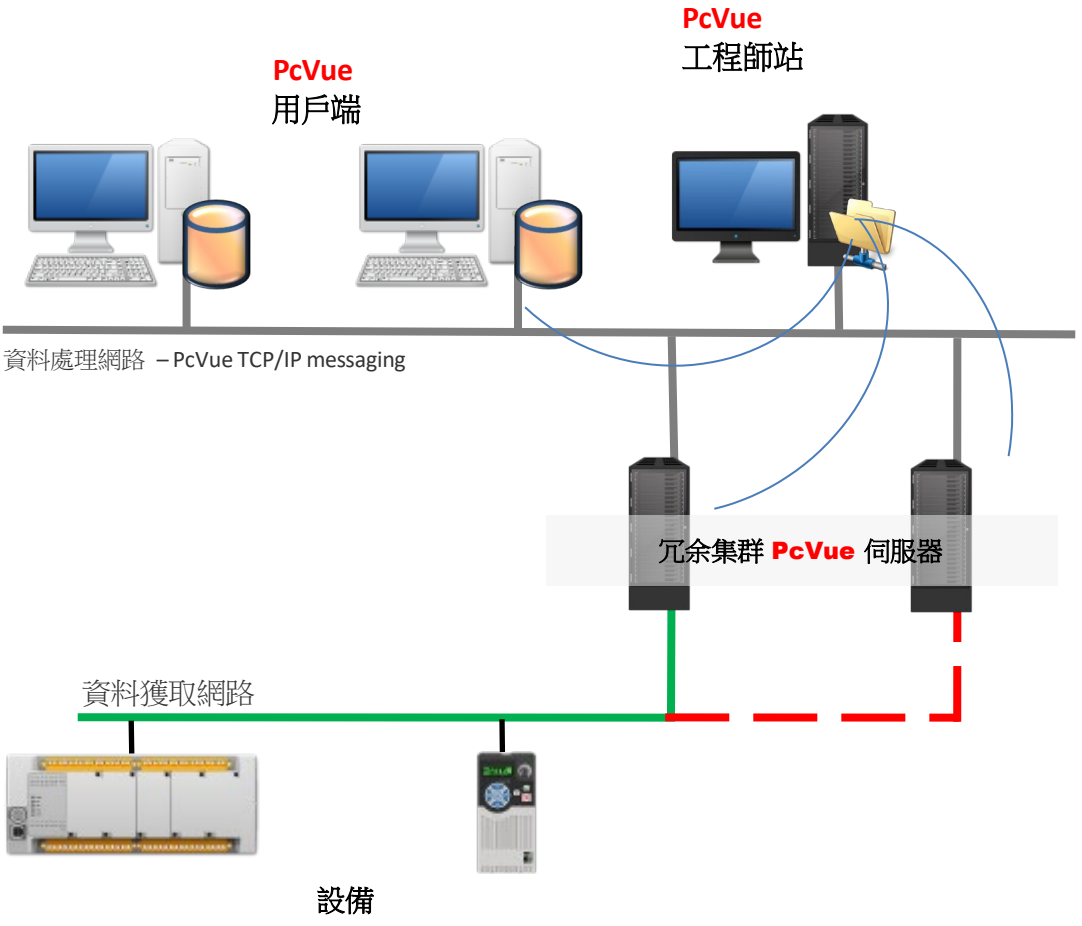
- 最大限度地減少用戶端的應用程式啟動時間
- 大幅減少網路上的資料負載

FrontVue可以連接多個OPC伺服器以便於：

- 連接到遠端本機伺服器以從任何特定設備檢索詳細資訊。
- 顯示來自多個PcVue伺服器的串聯事件，以在警報/日誌檢視器中向操作員顯示單個/唯一清單。

2.7 帶版本管理的工程師站

- ✓ 輕鬆維護和部署專案和/或庫
- ✓ 無限數量的版本
- ✓ 修改跟蹤
- ✓ 降低錯誤和丟失的風險



為了使專案的維護和部署更容易、更快，PcVue 提供了**內置的中央專案管理工具**。
不同版本的項目和/或庫集中在網路上的共用目錄中。 可以從網路上的任何工作站載入和修改它們。
通常，專用的 PcVue 工程師站用於託管中央版本目錄並對專案進行更改
任何工作站都可以手動載入和運行任何類型的版本，或者從中央專案目錄自動載入和運行專案和/或庫的一個參考版本。

支援的功能有:

- 3 種類型的版本：開發、操作和參考
- 版本的可配置內容
- 跟蹤每個版本的修改
- 自動版本編號系統
- 無限數量的版本（磁碟空間足夠大）

2.8 Web 和移動架構

本節介紹了為 PcVue 12 及更高版本部署基於 Web 和移動設備的架構的最佳方式和常見模式。

PcVue 12 在 Web 和移動組件的部署以及整合到 IT 環境中有幾項改進，特別是可以將 Web 伺服器層與工業網路分開。強烈建議利用這種新的職責分離功能，並在 DMZ 上與工業或 SCADA 網路隔離 Web 伺服器。但是這種方案不可能在所有系統中都適用，特別是在較小規模的系統中，這就是為什麼本節將重點放在各種不同的部署方案上：

- 獨立一體化設置的簡化方法，
- 大型企業 SCADA / HMI 系統，
- 遠端存取小型系統

2.8.1 EasyMobileTechnology

PcVue 的 Web 和移動解決方案採用專有的獨家技術 EasyMobileTechnology，允許設置沒有閘道/外掛程式的移動架構，嵌入所有必要的安全功能（https，OAuth，證書）和 HTML5 技術以及維護工具。

該技術符合以下標準：

- 沒有閘道，沒有額外的外掛程式
- 無需在用戶端上安裝任何軟體
- 簡單設置 – 無腳本 – 僅限嚮導
- 對協力廠商應用程式開放
- 適應任何用戶：最終用戶，SI，IT
- 安全可擴展的架構和通信
- 易於診斷

2.8.2 Web 部署控制台

Web 部署控制台是用於設置、部署和維護 Web 或移動架構的組件。
它支援以下功能：
：

- ✓ 在 IIS 上部署 Web 服務和 Web 應用程式
- ✓ PcVue Web 後端端點管理
- ✓ 資料保護管理
- ✓ 證書管理
- ✓ 使用者訪問日誌記錄和 OAuth 伺服器管理
- ✓ IIS 審核/診斷

Web 部署控制台運行在託管 Web 伺服器 IIS 的伺服器上。

2.8.3 Web 和移動用戶端

2.8.3.1 HTML5 Web 用戶端

WebVue 是一個使用 Web 流覽器和 Internet 或 Intranet 連接的 Web 用戶端，可以遠端顯示和控制 PcVue 專案。 具有適當使用者許可權（用戶名和密碼）的使用者可以從網路上的任何位置訪問 PcVue SCADA 應用程式。 WebVue 在 Web 流覽器中運行時獨立於作業系統，它直接顯示 PcVue 畫面，無需任何修改。
PcVue Web 伺服器和 WebVue 用戶端之間的通信使用 Microsoft IIS 技術和企業防火牆來管理安全性。

2.8.3.2 TouchVue – 帶報警和實際推送服務功能的移動 APP 應用

TouchVue 移動應用程式允許移動設備（平板電腦，智慧手機.....）通過 PcVue Web 伺服器的公共 Web 服務來訪問變數的即時值、不同的警報、歷史清單以及曲線趨勢。
例如，操作員可以確認警報或強制設定點等。

2.8.4 架構 #1: 一體化部署

- ✓ 單機一體化設置的簡化方法
- ✓ 安全性低
- ✓ 用於局域網且與外部訪問完全隔離的情況

2.8.4.1 介紹

在此部署方案中，PcVue Web 後端站和 Web 伺服器組件未分開。 它們在同一台電腦上運行。

Web 和移動用戶端（包括 WebVue 和 TouchVue）連接到與 Web 伺服器相同的網路。

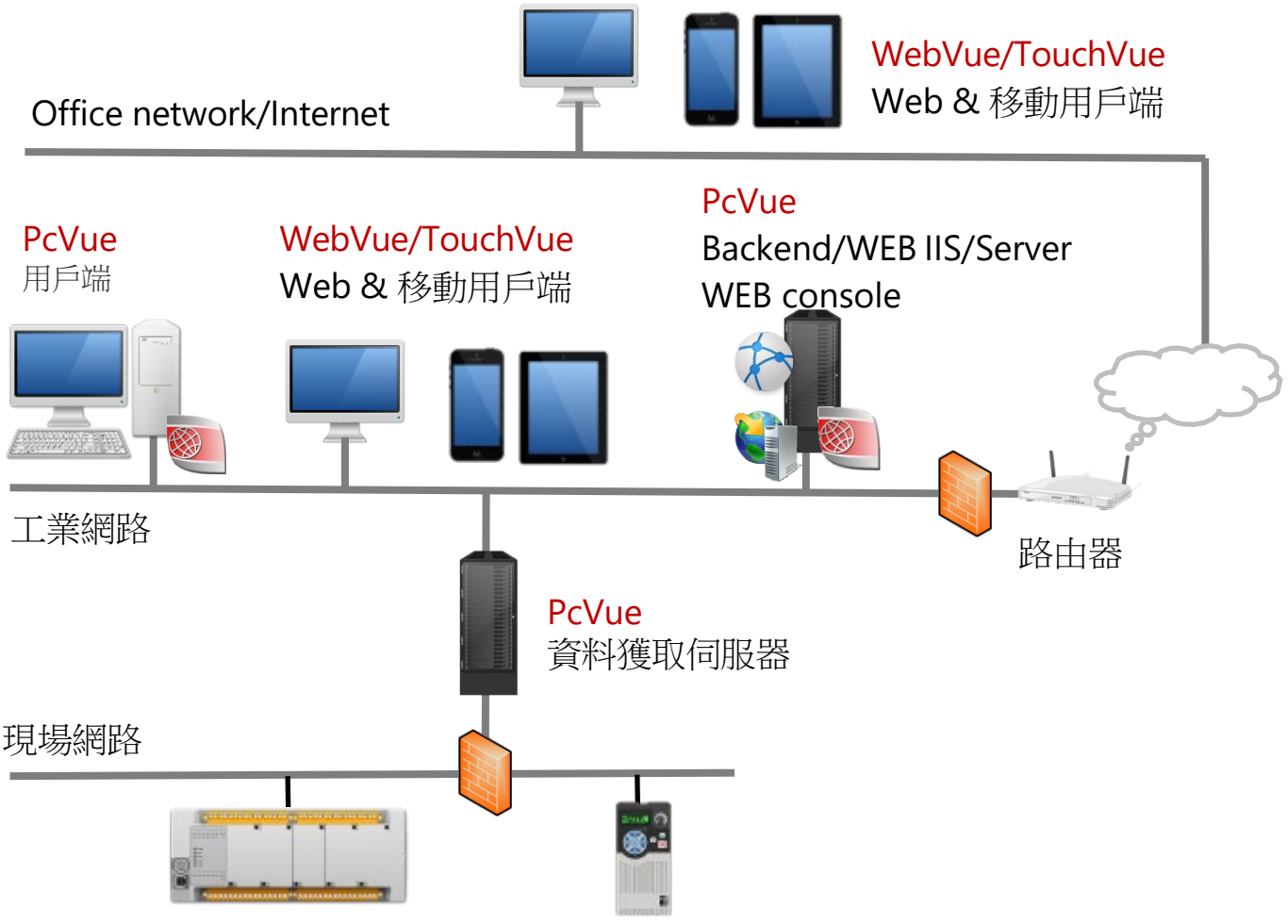


圖 1 – 架構#1 – 一體化部署

注意:

- 根據 RFC 6890 中描述的典型使用模式，IP 範圍和位址完全是為了說明需要，也可以使用任何其他子網範圍或位址集。
- PcVue SCADA 系統的架構完全是為了說明需要，可能與您的實際設置不同。
- 儘管建議將工業網路與自動化網路分離，但完全是為了說明需要。

2.8.4.2 什麼時候使用?

此架構適用於 Web 和移動用戶端與 PcVue Web 後端站位於同一子網上的部署方案。

當網路（子網）是私有的，並且與外部訪問完全隔離時，此部署方案的使用相當適合。 特別是操作人員使用的電腦和設備也不得訪問外部網路，以避免被用做訪問工業網路的入口。

2.8.4.3 什麼時候不適用?

當網路對來自外部網路的傳入請求開放或打開來自未知設備的不受保護的訪問時，請勿使用此方案。

特別是當需要從 Internet 上的 Web 和移動用戶端系統進行訪問時，不要使用此方案，也不建議使用其他網路安全手段（例如 VPN 隧道）。

2.8.4.4 要求

1. 此架構的部署需要最低水準的網路專業知識。
2. 要求所有電腦和移動設備位於同一子網上，通常是工業網路，包括 Web 和移動用戶端，Web 伺服器和 PcVue Web 後端站。
3. 此網路上的用戶端應該毫無保留地信任 Web 伺服器電腦，因為它們位於同一個網路上，並且根據定義，它是私有網路。
4. 此架構對 Web 伺服器憑證的可信賴性的最低要求起作用。來自憑證授權的證書不是強制與 Web 伺服器建立信任的證書。

2.8.4.5 優勢

1. 只需要一台電腦來託管 PcVue Web 後端和 Web 伺服器。
2. 此電腦不需要多個網卡。

3. Web 和移動用戶端直接使用 Web 伺服器電腦的 IP 位址連接即可訪問。

   Windows 平臺上的功能變數名稱解析不需要 DNS。 Web 伺服器電腦可以通過其主機名稱從任何基於 Windows 的 Web 用戶端進行定址。

   如果為有限數量的使用者提供服務，則可以在 PcVue Web Server 電腦上使用 Windows 桌面作業系統（如 Windows 10）。在所有情況下，強烈建議使用伺服器作業系統。
   使用非 Windows 用戶端設備（Android，iOS，Linux）時，DNS 伺服器的存在是名稱解析的必要條件。這可以通過使用用於 PcVue Web 後端站的 Windows Server 作業系統和啟動 DNS 伺服器角色來實現。

4. 自簽章憑證的使用是開箱即用的，但需要在 Web 用戶端中添加安全例外，或者在移動用戶端應用程式上啟用“忽略證書錯誤”選項。

   如果有可從網路訪問的 Active Directory 伺服器，則可以從 Active Directory 伺服器頒發域證書，並由域的所有用戶端（通過域策略或通過公司 MDM 系統）信任。

2.8.4.6 限制

1. 在 Windows 桌面作業系統上託管 Web 伺服器時會有限制。 特別是 IIS 可以處理的最大用戶端連接數是有限的。

2. 如果主機名稱不是 FQDN，Microsoft®Edge 不允許存儲 cookie。 這會導致 Web 元件出現問題。 可以通過將 URL 更改為：

   ```
   https://<hostname>.local
   ```

3. 當使用無效（部分受信任或不受信任）證書時，可能會遇到有限的性能，特別是在 WebVue 用戶端載入期間，因為在這種情況下，檔不會被 Web 流覽器緩存。

2.8.4.7 Web 部署控制台

可以使用 WDC 的“快速設置”嚮導將所有設置保留為其預設值，來輕鬆部署此架構。因此，WDC 需要與 PcVue Web 後端和 Web 伺服器安裝在同一台電腦上。

2.8.5 架構#2: 網路隔離和DMZ

- ✓ 大型企業 SCADA / HMI 系統
- ✓ 高水準的安全性
- ✓ 當 Web /移動用戶端位於工業網路之外時

2.8.5.1 Description 介紹

在此架構中，PcVue Web 後端站與 Web 和移動用戶端位於不同的物理或邏輯網路上，處於不同的安全範圍，需要與 DMZ 隔離。 內部網路（DMZ 路由器的 LAN 側）是專用安全網路。 外部網路（DMZ 路由器的 WAN 側）是不太受信任的網路，通常是公司辦公室網路或 Internet。

Web 伺服器元件託管在 DMZ 內的電腦上，PcVue 後端託管在安全網路上。

該架構提供了與 IT 網路的最佳集成，並允許最大程度地遵守 IT 指南和實踐。

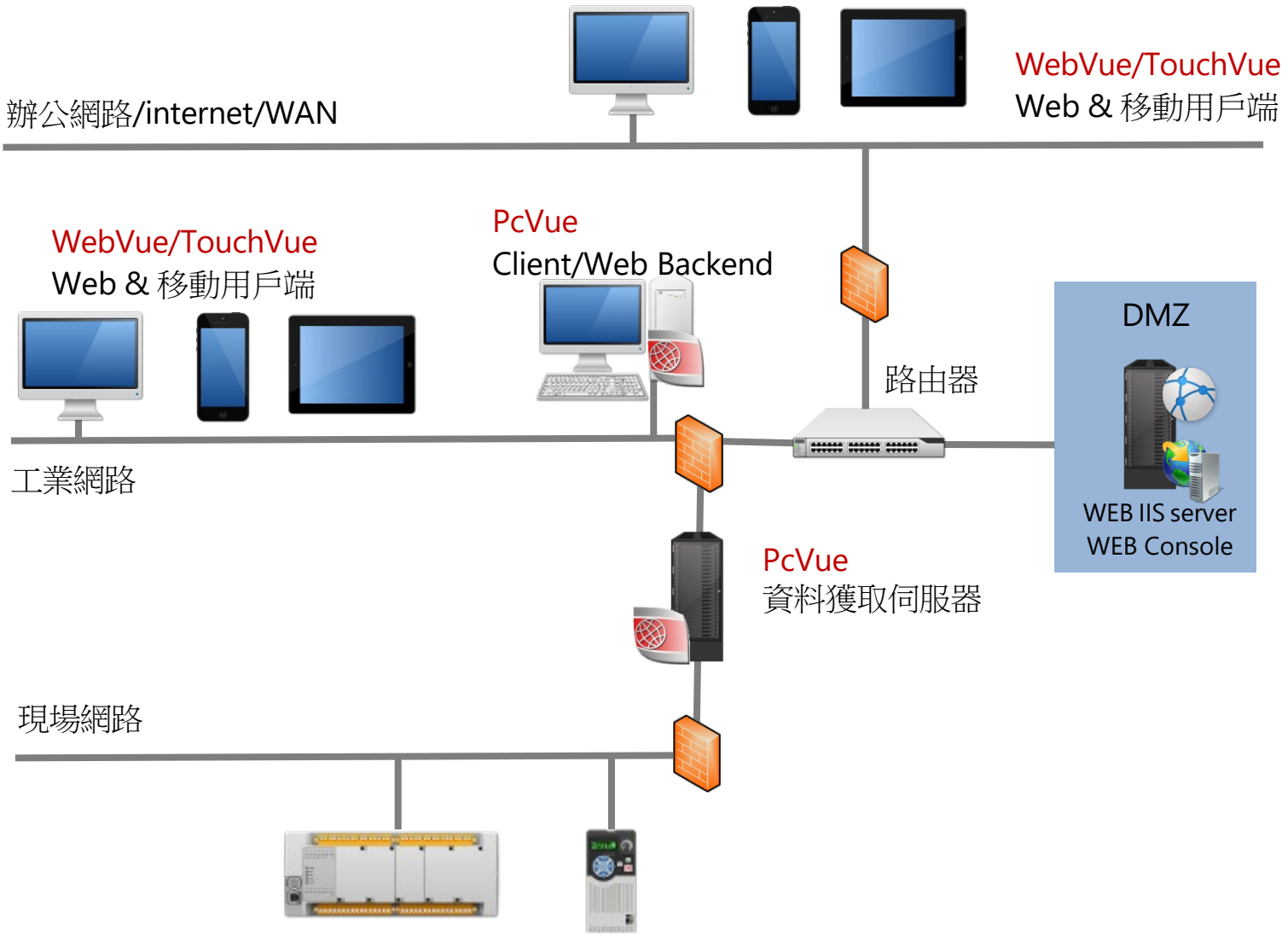


圖 2 – 架構#2 – 網路隔離和 DMZ

注意:

- 根據 RFC 6890 中描述的典型使用模式，IP 範圍和位址完全是為了說明需要，也可以使用任何其他子網範圍或位址集。
- PcVue SCADA 系統的架構完全是為了說明需要，可能與您的實際設置不同。
- 儘管建議將工業網路與自動化網路分離，但完全是為了說明需要。

2.8.5.2 什麼時候使用?

只要 Web 和移動用戶端不在安全的工業網路上，就建議使用此部署架構。

2.8.5.3 要求

1. 部署此架構所需的網路和 IT 專業知識水準從中級到高級。

2. 需要合適的網路架構來將私人網路絡與受保護較少的網路隔離開來。 這包括路由器（以及足夠的路由配置）和至少一個防火牆。

   支援常見的 DMZ 架構，包括單防火牆設置和雙防火牆設置：

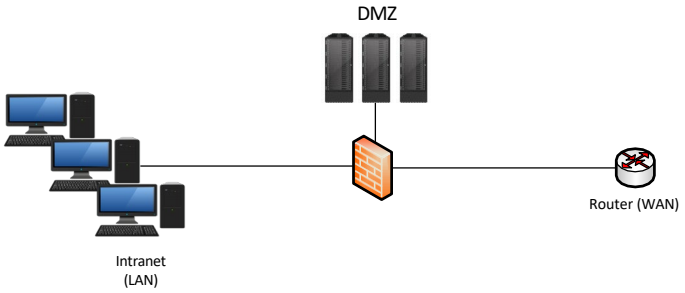


圖 3 - DMZ – 單防火牆設置

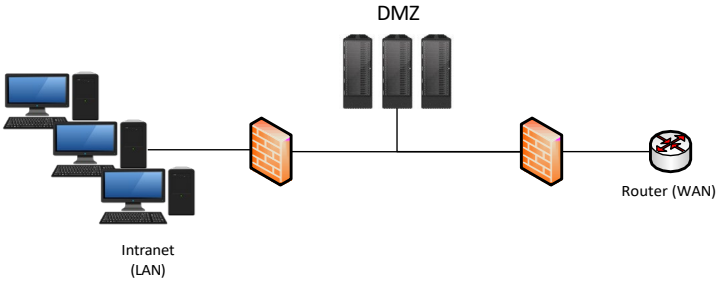


圖 4 - DMZ – 雙防火牆設置

3. 可能需要得到最終使用者的 IT 部門支援才能正確設置網路隔離、名稱解析和證書。

   這包括正確的配置：
   - DNS
   - 路由
   - NAT（或埠轉發）
   - 證書

   作為公司 PKI，可能需要 Active Directory 基礎結構來頒發證書並確保信任關係作為全域策略的一部分。

4. 為了驗證較小的可信網路上的 Web 伺服器電腦的身份並防止中間人攻擊，必須使用完全受信任的證書。

   - 此證書可由 IT 部門（公司網路 Active Directory 伺服器）頒發。如果所有 Web 和移動用戶端都與企業網路架構處於可信關係，那就足夠了。

   - 此證書可由 IT 部門通過可信 CA 頒發。如果 Web 伺服器是由外部 Web 和移動用戶端訪問的必要條件（用戶端設備/電腦與公司網路基礎架構不存在信任關係的典型訪問）。

   - 如果存在 Internet 訪問，且使用者組織策略允許 Let's Encrypt®服務，則可以通過 WDC 的 Let's Encrypt®嚮導發出此證書。

5. 較小的可信網路上需要能夠解析 Web 伺服器名稱的 DNS 伺服器。

6. Web 伺服器電腦上的 Windows Server 作業系統，理想情況下也位於 PcVue Web 後端站上。
7. 必須至少通過其 IP 位址訪問 Web 伺服器電腦上的 PcVue Web 後端站。由於 DMZ 記憶體在名稱解析的平均值，因此也可以通過主機名稱進行訪問：
   - Web 伺服器電腦的 hosts 檔中的專用條目。
   - 工業網路中可從 DMZ 訪問的 DNS 伺服器。

   如果尚未提供，則可以在 PcVue Web 後端站的 Windows Server 作業系統上啟動 DNS 伺服器角色。

   注意：允許從 DMZ 內的電腦訪問私人網路絡與 DMZ 常見模式和實踐相矛盾。但是，由於技術原因，需要向該埠打開 TCP 埠 8090。

2.8.5.4 優勢

1. 通過在完全合格的功能變數名稱下公開 Web 伺服器的 Web 和移動服務以及應用程式，該架構允許從不太可信的網路（通常是 Internet 或 Intranet）方便地訪問。
2. 它允許根據 IT 網路隔離做法對網路流量進行最大程度的控制，確保從外部網路到工業網路不存在不期望的傳入連接請求，包括網路周邊的流量控制和監控。

2.8.5.5 Web 部署控制台

可以使用任何 WDC 設置嚮導來部署此架構。 “快速設置”嚮導的默認設置並不適用於所有情況。WDC 需要安裝在 Web 伺服器電腦上。

2.8.6 架構#3: 用於遠端存取的簡化 NAT 方案

- ✓ 遠端存取小型系統
- ✓ 在沒有可用的託管 IT 架構時使用

2.8.6.1 Description 介紹

此部署方案對應於單個專用 LAN，即工業網路，其中 Web 伺服器，PcVue Web 後端站和大多數 Web 和移動用戶端都駐留在其中。專用 Internet 訪問用於遠端連接。
在此部署方案中，Web 和移動用戶端分佈在 NAT 邊界（本地和遠端 Web 用戶端）的兩側。

雖然這樣部署此架構在技術上是可行的，但不建議在不部署其他安全措施的情況下這樣做。

可行的方案包括 VPN 的使用和用戶端位址鎖定，在這種情況下，架構可能在邏輯上等於架構＃1。通過使用網路邊界的專用 DMZ 埠來建立私人網路段，在這種情況下，架構是架構＃2 的簡化版本。在任何情況下，建議將 PcVue Web 後端站和 Web 伺服器分開，如架構＃2 中所述，這本身就是一種額外的安全措施。
如果通過協力廠商提供 Internet 訪問並且需要由 ISP 提供和操作的機上盒等設備，則強烈建議安裝用於控制網路邊界的設備。特別提醒，強烈建議不要使用替代解決方案，例如“暴露主機”模式。

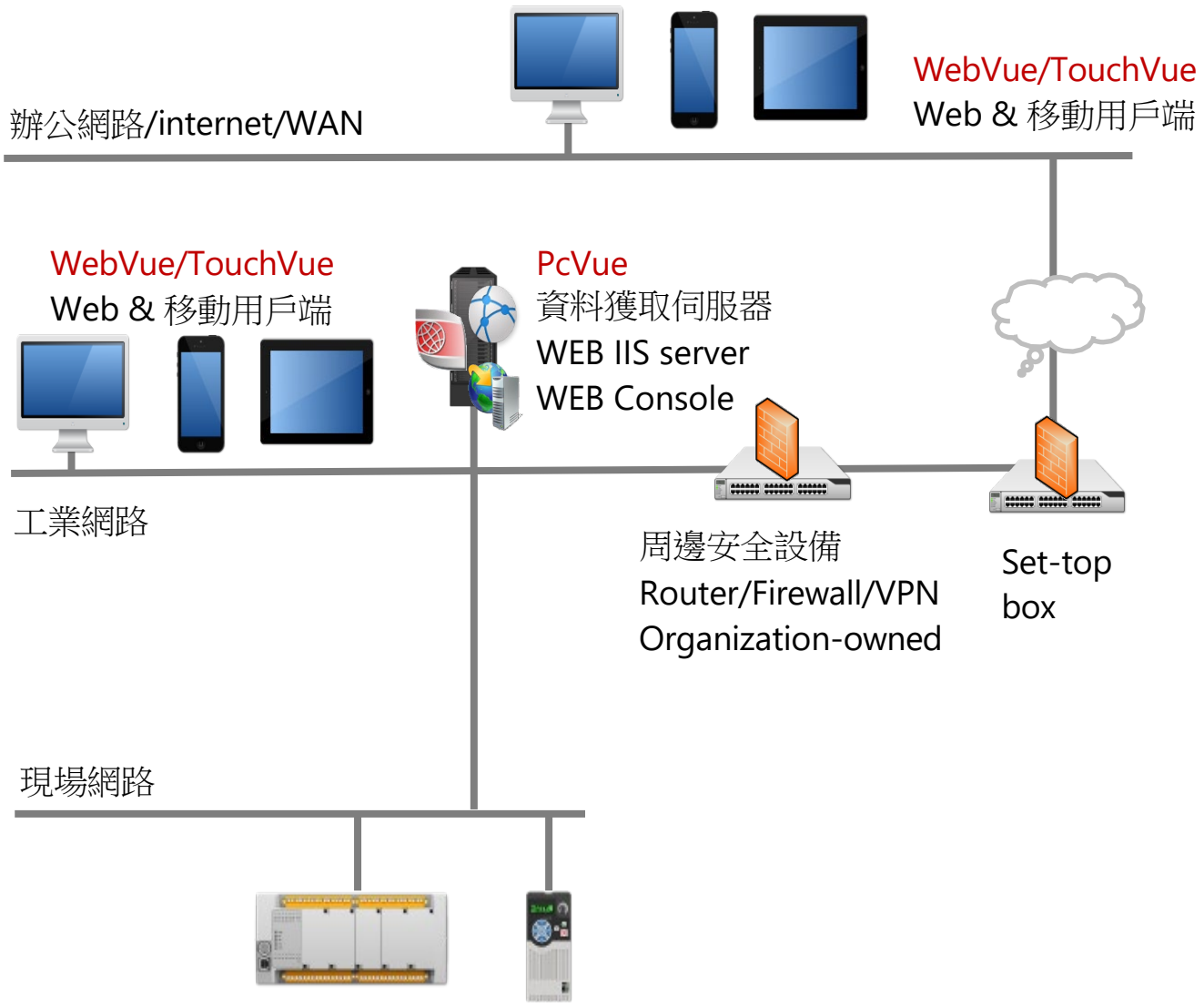


圖 5 – 架構 #3 – 用於遠端存取的簡化 NAT 方案

注意:

- 根據 RFC 6890 中描述的典型使用模式，IP 範圍和位址完全是為了說明需要，也可以使用任何其他子網範圍或位址集。
- PcVue SCADA 系統的架構完全是為了說明需要，可能與您的實際設置不同。
- 路由器設備暴露給 WAN 的 IP 位址可能取決於您的 ISP。
-

2.8.6.2 什麼時候使用?

當沒有可用的託管 IT 基礎架構時，可能需要此部署方案進行簡單的遠端存取。

我們建議使用此類架構運行舊版 WebVue 的現有系統遷移到架構＃2 或應用其他安全措施。

2.8.6.3 什麼時候不使用?

如果不瞭解與不良網路隔離和弱網路流量控制相關的風險，請不要在生產環境或現實系統中使用此架構。

2.8.6.4 要求

1. 部署此架構所需的網路和 IT 專業知識水準低至中等。

2. 用於在私人網路絡和受保護較少的網路之間建立連接的網路結構。用於連接路由器任一側的 Web / 移動用戶端的網路結構。

3. 在網路邊界上配置的網路位址轉譯（或特定埠轉發）。

4. 為了驗證較小的可信網路上的 Web 伺服器電腦的身份，並防止中間人攻擊，必須使用完全受信任的證書。

   - 此證書可由 IT 部門通過可信 CA 頒發。如果 Web 伺服器是由外部 Web 和移動用戶端訪問時必須要有（用戶端設備/電腦與公司網路基礎架構不存在信任關係的典型訪問）。

   - 如果存在 Internet 訪問，且使用者組織策略允許 Let's Encrypt®服務，則可以通過 WDC 的 Let's Encrypt®嚮導頒發此證書。

5. Web Server 和電腦必須可以從兩個網段訪問 Web Server 電腦。

   如果 Web 伺服器在同一 FQDN 下的兩個網段上都是眾所周知的，則可以實現這一點。

   如果不是這種情況，則需要 Web 和移動用戶端通過使用其 FQDN 直接連接到 Web 伺服器電腦而不必使消息必須離開私人網路絡。在這種情況下，建議使用 NAT Loopback / Hairpinning。

如果這些選項都不可能滿足，建議通過 WDC 創建兩個不同的網站，這兩個網站都連接到同一個 PcVue Web 後端站

2.8.6.5 優勢

1. 該架構允許方便地訪問位於工業網路和 Internet 上的 Web 和移動用戶端。
2. 此架構是提供遠端 Web 訪問的老 WebVue 系統遷移過程的第一步。

2.8.6.6 限制

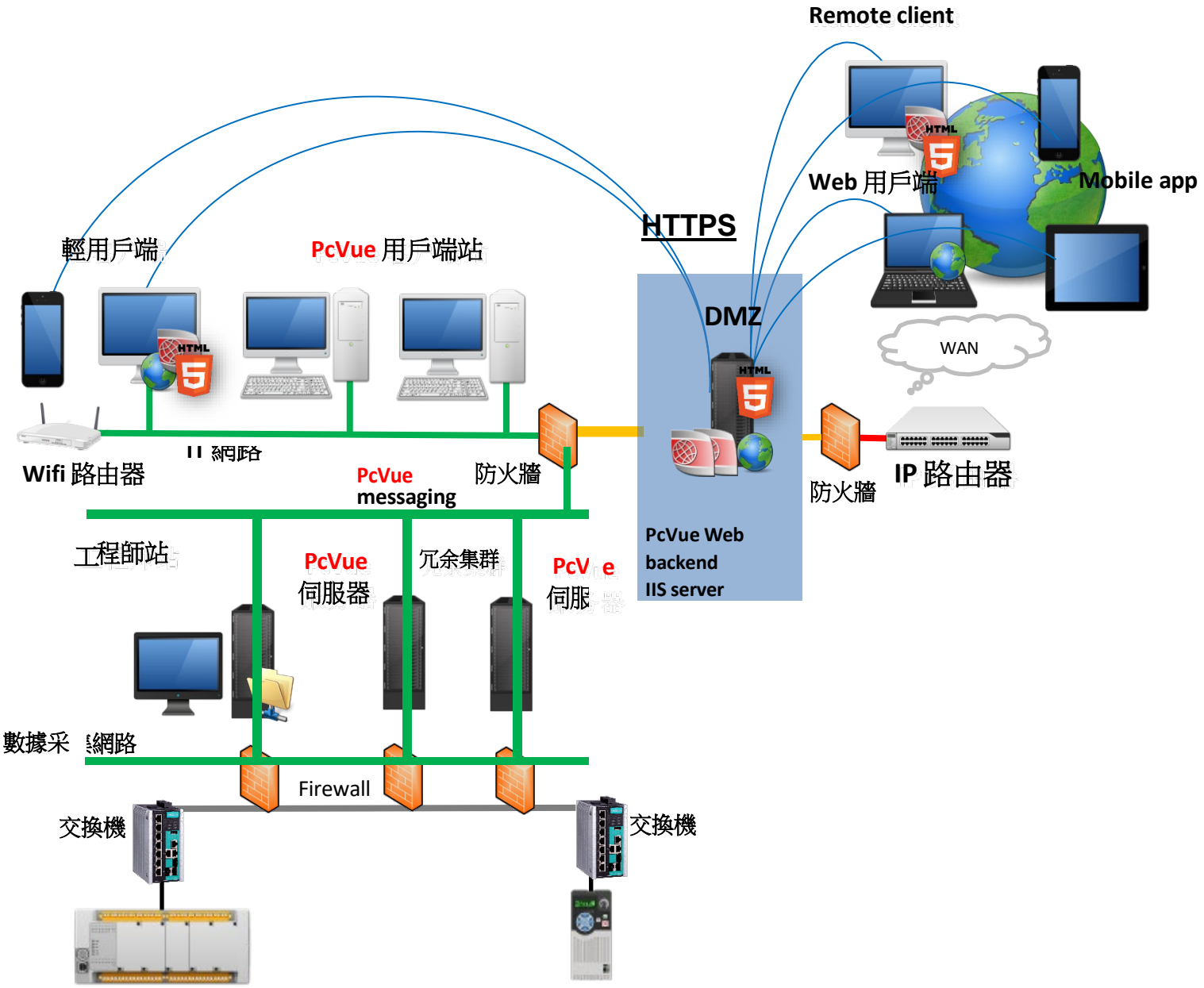
如果未添加特定設備來控制網路邊界，則此部署方案提供有限的網路安全性，因為：

- 您依靠 ISP 擁有的機上盒來控制網路邊界和遠端連接，
- 作為工業控制系統一部分的電腦直接暴露於互聯網。

在最糟糕的情況下，攻擊者可利用多個級別上的潛在安全性漏洞來訪問工業控制系統。

2.8.6.7 Web 部署控制台

可以使用任何 WDC 設置嚮導來部署此架構。WDC 需要安裝在 Web 伺服器電腦上。



2.9 混合架構

此架構的示例取決於下麵的元素：

- 資料獲取由工業網路上的複聯採集伺服器執行。
- 開發站用於專案的集中管理。
- 操作在用戶端站上執行，用戶端位於防火牆隔離的電腦網路上.

- 安裝在防火牆隔離的控制區（DMZ）中的 Windows 伺服器上的工作站，託管 Web 伺服器，移動伺服器和 Windows RDS 伺服器。
- 可以使用 Windows 遠端存取元件通過 RDS 實例遠端運行用戶端。
- 安裝在伺服器上的介面允許在支援 HTML5 的任何設備上顯示用戶端實例。
- Web 用戶端允許從標準 Web 流覽器進行操作。
- 連接到移動伺服器的移動應用程式用於通過智慧手機或平板電腦通知和確認警報和控制。
- Web 伺服器和終端之間的交換使用安全通訊端 HTTPS。
- Windows Active Directory 管理整個系統的使用者訪問，以進行單點登錄（SSO）

必須採取一些預防措施來保護PcVue多層架構的元件。

所以必須：

- 通過創建需要相同安全級別的VLAN來劃分各種網路（例如電腦和工業）

- 使用防火牆過濾資料。

使用DMZ和路由器還允許將網路與外部隔離並防止不必要的入侵。

為了保護兩個網路元件之間的通訊流量，也可能需要建立VPN隧道解決方案。 通常，可以在PcVue採集站和通過TCP / IP通信的PLC之間建立VPN，或者在與多個遠端監控網站之間建立VPN。

PcVue Solutions與MOXA合作，提供完整的硬體保護解決方案，以解決上述問題：

-全系列安全的工業防火牆/ VPN
- 不同網路區域之間的流量限制和控制
- 創建流量限制

2.10 虛擬化

- ✓ 減少物理站的數量
- ✓ 減少管理工作量和成本
- ✓ 低成本的精簡型用戶端
- ✓ 在精簡型用戶端上免費安裝
- ✓ 符合 IT 要求

虛擬化在計算中是指創建某物的虛擬（而非實際）版本的行為，包括但不限於虛擬電

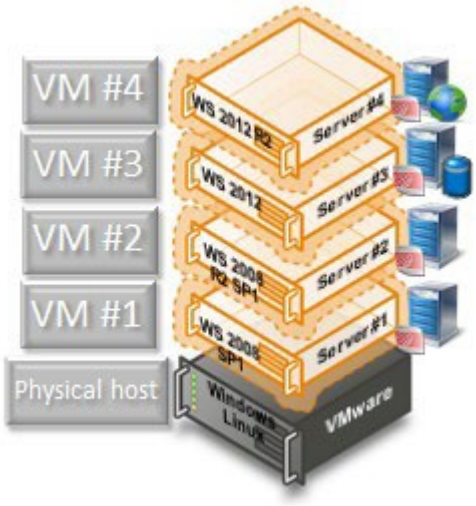
腦硬體平臺，作業系統（OS），存放裝置或電腦網路資源。

硬體虛擬化或平臺虛擬化是指創建一個虛擬機器，其功能類似於具有作業系統的真實電腦。 在這些虛擬機器上執行的軟體與底層硬體資源分離。
在硬體虛擬化中，主機是發生虛擬化的實際機器，而客戶機是虛擬機器。 單詞“host”和“guest”用於區分在物理機器上運行的軟體與在虛擬機器上運行的軟體。
工業應用程式的虛擬化可以使許多相關部門受益：IT、工程和運營。

2.10.1 應用虛擬化

✓ VMWare 主機可以在隔離環境中運行不同版本的 PcVue 或 FrontVue
✓為一次性操作設置工作環境變得容易
✓可以建立一個老的作業系統
✓在 Windows 7，Windows 8，Windows 8.1，Windows 2008 SP2 和 2008 R2 SP1, 2012 和 2012 R2 Server 和 VMWare 下運行

2.10.2 資源虛擬化

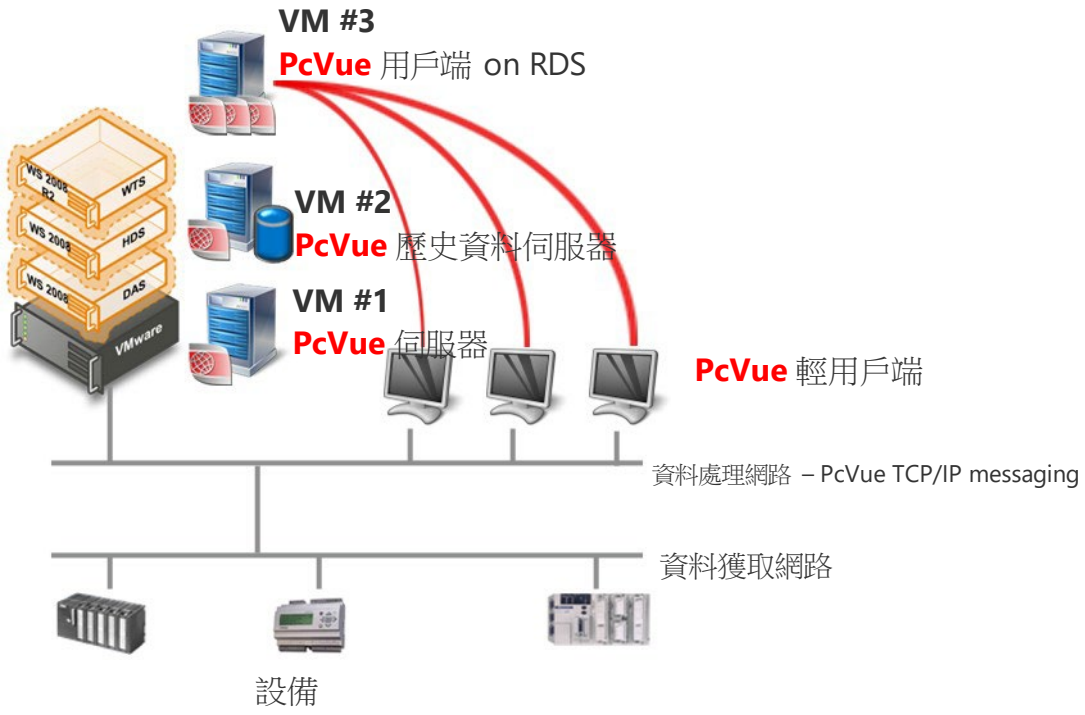


✓虛擬化環境可以在單個物理機器上的不同作業系統下運行各種PcVue伺服器

✓PcVue許可證可以是不同類型的

✓根據資源優化規則將虛擬機器動態分配給物理主機

2.10.3 部署示例



SCADA應用程式在IT管理站上運行。 運行VMware的單個物理機器或同等主機託管隔離虛擬機器中的所有站，其中一個VM運行RDS，允許多個RDS用戶端站連接到伺服器。 本文中描述的大多數架構都可以部署在虛擬環境中。

3. 專有詞彙

名稱	縮寫	介紹
Microsoft® Internet Information Services	IIS	Internet 資訊服務（IIS）是由 Microsoft®創建並隨 Windows 作業系統一起提供的 Web 伺服器。 IIS 是Microsoft®Windows 作業系統上的內置 Web 伺服器。
PcVue Web back end station		工業網路上的 PcVue 站用作 PcVue 多站系統和實際 Web 伺服器（IIS）之間的閘道。 Web 後端運行 Sv32.exe，即 PcVue 主進程。
Web Server machine Web Server computer		運行 IIS Web 伺服器的電腦，該電腦又託管 PcVue Web 伺服器元件。 Web 伺服器不運行 Sv32.exe（PcVue 主進程本身）.
PcVue Web Server Components		在 Web 伺服器電腦上安裝的一組服務和應用程式，用於連接 PcVue 的 Web 和移動用戶端。
Web & Mobile Client Systems		在智慧移動設備上在 Web 流覽器或本機移動應用程式（如 TouchVue）中運行 WebVue Web 用戶端的電腦和設備。
Web Deployment Console	WDC	安裝在 Web 伺服器電腦上的桌面應用程式，允許系統管理員配置、部署和監視 IIS 和 PcVue Web 伺服器元件。
Industrial Network		包含 PcVue SCADA 網路的網段。 在 ANSI / ISA-95 資訊模型（也稱為 SCADA 級別）中稱為 2 級工業網路
Demilitarized Zone	DMZ	DMZ 或非軍事區 - 有時稱為遮蔽式子網路 - 是一個物理或邏輯網路，它包含並向組織的不受信任的網路（通常是更大的網路，如 Internet）公開面向外部的服務。 DMZ 的目的是為組織的局域網（LAN）添加額外的安全層。
Fullly Qualified Domain Name	FQDN	一個功能變數名稱，指定其在網域名稱系統（DNS）的樹層次結構中的確切位置。 它指定所有域級別，包括至少一個二級域和一個頂層網域。
Domain Name System	DNS	DNS 是用於連接到 Internet 或私人網路絡的電腦、服務或其他資源的分層分散命名系統。
Windows Internet Name Service	WINS	WINS 是Microsoft®的 NetBIOS 名稱服務（NBNS）的實現，它是 NetBIOS 電腦名稱的名稱伺服器和服務。
Subnetwork	Subnet	子網是 IP 網路的邏輯細分。 屬於子網的電腦在其 IP 位址中使用通用、相同、最重要的位組進行定址。 當源位址和目標位址的路由首碼不同時，通過路由器在子網之間交換流量。 路由器充當子網之間的邏輯或物理邊界。
Virtual Private Network	VPN	虛擬私人網路絡（VPN）通過公共網路擴展私人網路絡，並使用戶能夠跨共用或公共網路發送和接收資料，就好像他們的計算設備直接連接到私人網路絡一樣。
Firewall		它是一個網路安全系統，它根據預定的安全規則監視和控制傳入和傳出的網路流量。
Network Address Translation	NAT	NAT 是一種通過修改資料包的 IP 報頭中的網路位址資訊將一個 IP 位址空間重新映射到另一個 IP 位址空間的方法，同時它們通過流量路由設備傳輸。 NAT 閘道的一個可聯網路由的 IP 位址可用於整個私人網路絡。

名稱	縮寫	介紹
Port Forwarding	PAT	埠轉發或埠映射是網路位址轉譯（NAT）的應用程式，當資料包穿過網路閘道（例如路由器或防火牆）時，它將通信請求從一個位址和埠號組合重定向到另一個。 此技術最常用於通過將通信的目標 IP 位址和埠號重新映射到駐留在閘道（外部網路）另一側的主機上的受保護或偽裝（內部）網路上的主機上進行服務。
Internet Service Provider	ISP	Internet 服務提供者（ISP）是一種提供訪問，使用或參與 Internet 的服務的組織。
Private Key Infrastructure	PKI	公開金鑰基礎結構（PKI）是創建、管理、分發、使用、存儲和撤銷數位證書以及管理公開金鑰加密所需的一組角色、策略和過程。
Certificate Authority	CA	憑證授權或憑證授權（CA）是頒發數位憑證的實體。 CA 可以是受信任的協力廠商，也可以是公司 PKI 的一部分。
Mobile Device Management	MDM	移動設備管理是移動設備管理的行業術語，例如智慧手機，平板電腦，筆記型電腦和臺式電腦。 MDM 主要處理企業資料隔離，保護電子郵件，保護設備上的公司文檔，實施公司策略，集成和管理移動設備。
Hypertext Transfer Protocol Secure Hypertext Transfer Protocol	HTTP / HTTPS	超文字傳輸協定（HTTP）是用於分散式，協作式和超媒體資訊系統的應用程式通訊協定。 HTTP 是萬維網資料通信的基礎。 HTTPS（安全的 HTTP）是用於安全通信的超文字傳輸協定（HTTP）的擴展。 該協議通常稱為 HTTP over TLS 或 HTTP over SSL。
Hairpinning		Hairpinning（也稱為“NAT 環回”）描述了使用其映射端點在同一 NAT 設備後面的兩個主機之間的通信。 Hairpinning 是 LAN 上的機器能夠通過 LAN /路由器的外部 IP 位址訪問 LAN 上的另一台機器（在路由器上設置埠轉發以將請求定向到 LAN 上的適當機器）。
WebSocket(s)		WebSocket（RFC 6455）是一種電腦通信協定，通過單個 TCP 連接提供全雙工通信通道。 WebSocket 旨在通過 HTTP 埠 80 和 443 工作，以及支援 HTTP 代理和仲介。 HTTP WebSocket 通過其 wss 綁定（Web Socket Secure）支持加密。
HTTP/2 - SPDY protocol		HTTP / 2 是 HTTP 網路通訊協定的主要修訂版。它源於早期的實驗性 SPDY 協定。 協議演進所帶來的主要改進通過引入減少的延遲、報頭壓縮、TCP 多工和請求流水線來關注網站的回應性。

一些通用定義來自維琪百科。無法保證準確性或適用性。

PcVue Solutions

ARC Informatique

Headquarters and Paris offices
2 avenue de la Cristallerie
92310 Sèvres - France

tel + 33 1 41 14 36 00
fax + 33 1 46 23 86 02
hotline +33 1 41 14 36 25
arcnews@arcinfo.com
www.pcvuesolutions.com

GERMANY - Munich
PcVue Gmbh

Italy - Milan
PcVue Srl

UK – London control
Technology International

USA - Boston
PcVue Inc.

Chile - Santiago
PcVue Chile

SINGAPORE - Singapore
PcVue Sea

MALAYSIA- Kuala Lumpur
PcVue Sdn Bhd

CHINA- Shangai
PcVue china

JAPAN - Nagoya
PcVue Japan

UAE - Dubaï
PcVue DMCC

ISO 9001 and ISO 14001 certified

ARC Informatique

Private limited company capitalized
at 1 250 000 €
RCS Nanterre B 320 695 356
APE 5829C
SIREN 320 695 356
VAT N°FR 19320695356

PcVueSolutions 架構和部署