技术白皮书

PcVueSolutions 架构和部署

Last update :	May 2019
Revision :	7
Content :	介绍PcVue 解决方案的架构和部署
Confidentiality :	公开

PcVue® Solutions

目录

1.1 架构 2
1.2 角色 3
1.3 架构图例 4
1.3.1 图例 *4*
2.1 单机站 7
2.2 多站 8
2.3 带远程桌面服务器的多站-用于部署客户端工作站 9
2.4 高可用性 11
2.4.1 实时服务器冗余 *12*
2.4.2 单主动采集服务器模式 *12*
2.4.3 历史服务器冗余 *12*
2.5 多重冗余服务器 14
2.6 多层架构 15
2.6.1 多层架构：部署#1 ..... *16*
2.6.2 多层架构：部署#2 ..... *17*
2.7 带版本管理的工程师站 19
2.8 WEB 和移动架构 20
2.8.1 EasyMobileTechnology *20*
2.8.2 Web 部署控制台 *21*
2.8.3 Web 和移动客户端 *21*
2.8.4 架构 #1: 一体化部署 *22*
2.8.5 架构#2: 网络隔离和 DMZ *25*
2.8.6 架构#3: 用于远程访问的简化 NAT 方案 *29*
2.9 混合架构 33
2.10 虚拟化 34
2.10.1 应用虚拟化 *35*
2.10.2 资源虚拟化 *35*
2.10.3 部署示例 *36*

1. 概况

此文档介绍了部署监控软件的一些选项。
部署是将角色分配给工作站和服务器以满足给定实际网络架构中的系统要求的过程。
出于本主题的目的，我们将考虑监控软件具有以下主要功能：

- **数据采集** - 数据采集 – 使用 Modbus，OPC 等通信协议收集实时数据，表示实际值或计算值...
- **历史数据归档** – 记录实时数据，以便以后可以由主管本身或第三方应用程序访问。
- **报警** – 报警的生成和管理。
- **HMI** – 人机界面，作为表示层的图形界面，使操作员能够与监控系统进行交互。
- **多站** – 监控软件在网络架构中的站点之间分配实时和历史数据的机制。
- **Web 服务器扩展** – 用于将监控软件核心架构与 Web 客户端连接的一组组件。
- **和第三方系统的接口** – 比如 CMMS, GIS, ERP, MES...

实现功能和角色分配依赖于授权。 有关授权的更多信息，请联系当地的销售代表。

1.1 架构

典型架构如下：

- **单机版** – 所有SCADA功能都集成在一个工作站中。

- **多站架构** – 基于客户/服务器架构的SCADA。

- **高可用性架构** – 分布式SCADA功能和角色，以提供更好的弹性和可扩展性。 多站部署包括以下特定方案：
  - **数据采集冗余** – 两个或多个站配置为冗余（热备用）。
  - **历史数据冗余** – 两个或多个站配置为冗余（热备用）。
  - **互联服务器**。

- **三层架构** – 使用一个或多个站作为网关

- **工程师站** – 带有版本管理功能。

• Web & mobile – Web后端服务器以及基于Web和移动客户端。

1.2 角色

上述架构需要分配一下角色：

- **数据采集**
  - 与现场设备通信，
  - 实时数据和报警生产，
  - 为其他站提供实时数据和警报。
- **历史数据**
  - 使用其他站产生的实时数据和警报，
  - 处理数据存储，记录和重放历史数据，
  - 管理与 RDBMS 的连接，
  - 将历史数据提供给其他站。
- **Web 后端服务器**
  - 使用其他站产生的实时数据和警报，
  - 使用其他站保存的历史数据，
  - 管理与 IIS 的接口，
  - 为 Web 客户端提供服务，包括 WebVue 客户端，TouchVue 客户端，WebScheduler 和 Web Services Toolkit 客户端
- **网关**
  - 用于在两个网络之间安全地传输数据
  - 在一个网络上消耗其他电台产生的实时数据，警报和历史数据，
  - 为另一个网络上的站点提供实时数据，警报和历史数据。
- **HMI**
  - 向用户显示模拟，图形，报警查看器，日志查看器，趋势查看器...

根据角色的组合，监控软件的工作站可以更好地部署在桌面操作系统或服务器操作系统上。

1.3 架构图例

1.3.1 图例

HTML5

防火墙

Web 后端服务器

专利型归档单元

HDS 归档单元

单机站

PcVue 访问

服务器站

客户端站

中央版本文件夹

FrontVue

PcVue 实例

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. 架构示例

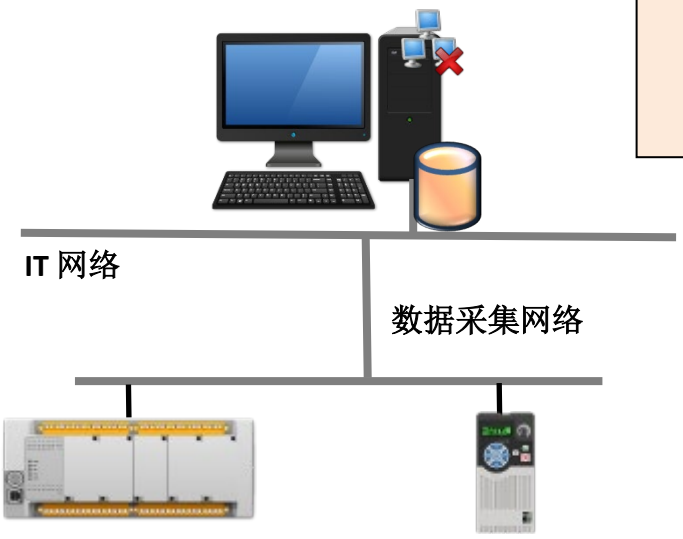
本主题描述了最常见的基本架构。根据以下因素，有许多变化可以满足系统要求

- 用户数量
- 操作员站的类型和数量（HMI）
- 可用性
- 灵活性
- 可扩展性
- 恢复力
- 维护和应用程序生命周期管理

请联系技术支持以获取更多信息。

2.1 单机站

- ✓ 最简单的架构
- ✓ 全部监控集中在“一体化”的工作站上
- ✓ 单机 PcVue 站负担所有功能



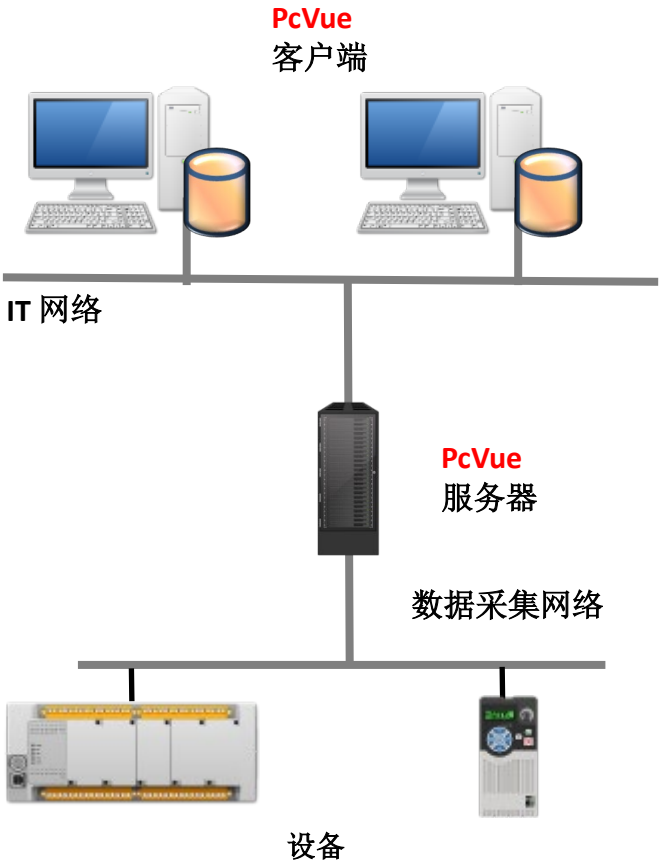
独立站通常是操作员直接操作，它是最简单的架构，所有功能和角色都集成在一个站中

在传统的单用户配置中，PcVue 监视和/或控制工业网络上的所有设备，并且还处理用户请求。 PcVue 可以在单个站上支持数万个变量。
PcVue 单机站是一个一体化的独立 HMI 站，使用 PcVue 的标准功能监视和控制您的项目：

- ✓ 数据采集，
- ✓ 实时数据库，
- ✓ HMI，
- ✓ 归档，
- ✓ 警报和日志，
- ✓ 趋势，
- ✓ 数据处理，报表
- ✓ 用户管理

2.2 多站

- ✓ 最简单的多站架构
- ✓ 从几个远程用户站监控项目
- ✓ 优化数据处理网络负载



最简单的客户端/服务器架构，适用于需要多个用户工作站与工业网络连接的应用程序。
服务器是与设备通信并将数据广播到客户端（或消费者）站的数据源站（生产者）。
PcVue 站之间的通信异步工作，并使用 PcVue TCP/IP 消息传送数据包中的数据。
服务器站可以仅是完整的用户操作站或数据采集服务器。它执行项目的所有数据处理。 历史数据归档可以仅在服务器端上实现，也可以在每个客户站的本地实现。
客户端可以使用任何支持 TCP/IP 并保证足够带宽的媒体连接到位于另一个位置的服务器，包括拨号网络，甚至是卫星链路。

通常是在 2 个不同的服务器上分别实现变量的数据采集和历史数据存储，或让客户端在本地存储历史数据。

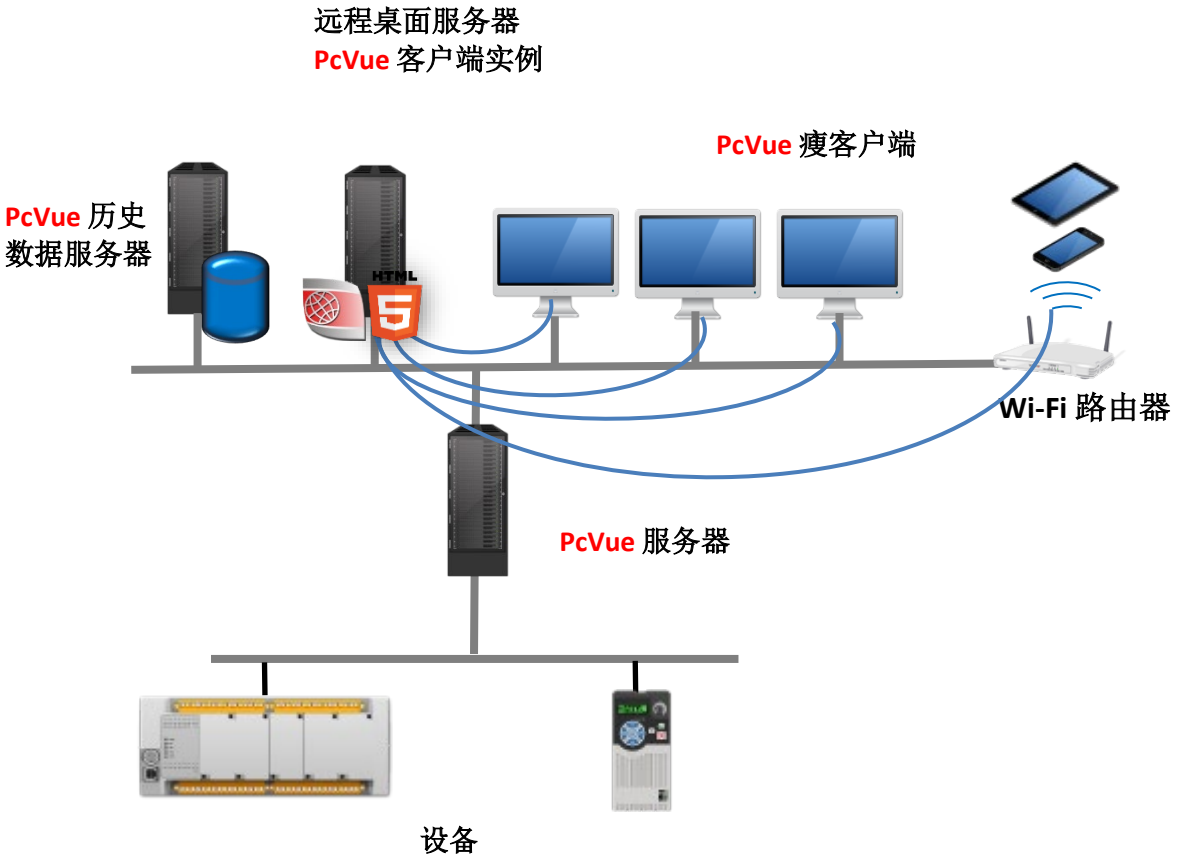
2.3 带远程桌面服务器的多站-用于部署客户端工作站

- ✓ 减少管理工作量和成本
- ✓ 低成本的瘦硬件客户端
- ✓ 在瘦客户端上免费安装

Windows Server 配置了远程桌面服务时，允许多个用户同时使用单个服务器的资源并执行服务器上安装的应用程序。用户通过网络连接到服务器的瘦客户端（也称为终端）与应用程序交互。以这种方式连接到 Windows Server 的用户的过程称为远程桌面会话，并使用称为远程桌面协议（RDP）的标准。瘦客户端（包括 Linux 或 Unix 下的 Wyse Thin Computing 终端）使用 RDP 客户端软件来管理 RDP。

除了使用远程桌面运行会话外，Windows Server 还使用本地监视器，键盘和鼠标运行会话。这称为本地会话（或有时称为控制台会话或交互式会话）。

在 RD 会话主机服务器上运行监控软件时，可以从每个远程桌面会话和/或本地会话运行监控软件的实例。仅安装了监控软件的一个副本。



从监控软件的网络角度来看，这种架构与之前的架构相同，只是作为合理化部署的一种方式使用客户站，RDS 和轻量级终端。

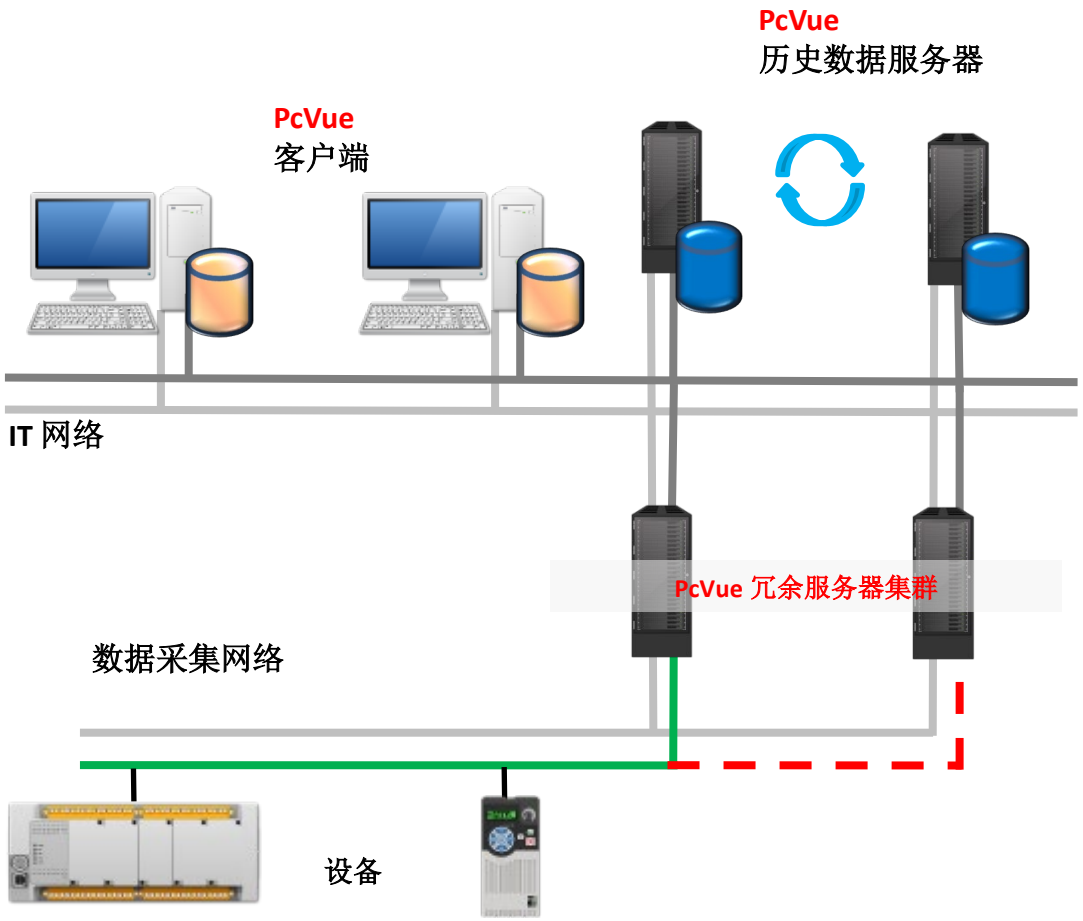
在此示例中，PcVue 客户端安装在 Windows Server 作为远程桌面服务器（RDS）运行的工作站上。

此工作站是 RD 会话主机服务器并托管 PcVue 客户端实例。用户可以从任何瘦客户端打开远程桌面会话并运行 PcVue 客户端实例。服务器上的 HTML5 接口允许任何配备符合 HTML5 标准的 Web 浏览器的瘦客户端通过 RDS 实例访问 PcVue 应用程序。

只有一个 PcVue 服务器也可以驻留在 RD 会话主机服务器上。
必须将 RD 会话主机服务器配置为承载多个客户端实例，以支持所需数量的同时会话。
瘦客户端不需要任何特定安装，这有助于现场部署应用程序。

2.4 高可用性

- ✓ 非常高的安全性和系统/数据可用性
- ✓ 使用双网络及安全的客户端 – 服务器设置
- ✓ 多用户站
- ✓ 优化的数据处理和现场网络数据负载



当需要更高的可用性和弹性时，这种更加分散的体系架构可以带来冗余和角色分离。它类似于多站架构，但具有数据采集服务器和历史数据服务器分离和冗余。
站之间可以使用双网络（LAN 和/或 WAN），现场网络也可以使用双网络。这样在任何客户站和数据源站之间有两条独立的网络路径。每个 PcVue 客户端站与每个服务器站之间保持两个连接通道，并且仅当这两个连接通道都不可用时才会尝试进行服务器之间的切换。
在工业以太网网络中，PcVue 可以管理通信介质冗余和设备冗余。
每个工作站都可以归档数据，以提高历史数据的可用性。

通常其他架构还包括 Web 服务器和 Web 客户端。

2.4.1 实时服务器冗余

实时服务器专用于采集 PLC 的数据并实时更新客户站的实时数据。 客户端站拥有图形界面，用于监视和控制项目。
这两台服务器之间是冗余的，并为客户站提供实时数据。

2.4.2 单主动采集服务器模式

服务器以单主动采集服务器模式运行。与工业网络通信的服务器称为“主动”。另一台服务器称为“被动”。只有主动服务器和 PLC 通信，为客户端站提供实时数据并同步被动服务器。
在主动服务器发生故障的情况下，被动服务器激活其与 PLC 通信并提供数据给客户端站。热备切换完成并且完全无缝地与操作员进行切换。
当启动服务器时，有两种可能的情况：
•其他服务器不工作。新服务器启动工业网络上的通信以刷新其设备变量并成为主动服务器。网络中的所有客户端都会自动订阅变量。
•另一台服务器已在运行并处于主动状态。新服务器自动变为被动并与活动服务器同步。
当被动服务器变为主动状态时，工业网络上的通信恢复立即生效，这使新的主动服务器立即运行。
主动服务器在时间 T 通过事件自动触发客户站。对于操作员来说，访问信息（控制/命令/确认/存档...）在任何站都是相同的;无论网络状态如何，数据来源都完全透明。
根据用户配置文件，可以从任何客户端工作站访问全部或部分站数据点。
在任何站点都可以知道所有网络站的状态和采集系统上的通信。该系统提供了一个完整的架构图，可以实时显示与其连接的 PLC 和组态软件。
系统可以根据授权，对冗余状态进行切换，实现服务器维护。（例如：强制被动服务器变为主动状态）。

2.4.3 历史服务器冗余

2.4.3.1 带两个同步数据库的模式

两台历史服务器在两个独立的 SQLServer 关系数据库上并行记录信息。两台服务器同时记录相同的信息。
先前可配置的日期范围信息将自动清除，通过这种方式控制数据库的大小，与保存长时间的数据相比，这样可以保证更快的访问时间。
如有必要，可以从 ASCII 文件中提取已清除的记录以“备份”。
定期自动合并缺失的信息以管理可能的系统停止（故障或维护）情况。这种合并是横向完成的：第一台服务器在第二台服务器上提取其缺失的历史记录，反之亦然。在合并结束时，关系数据库是相同的。

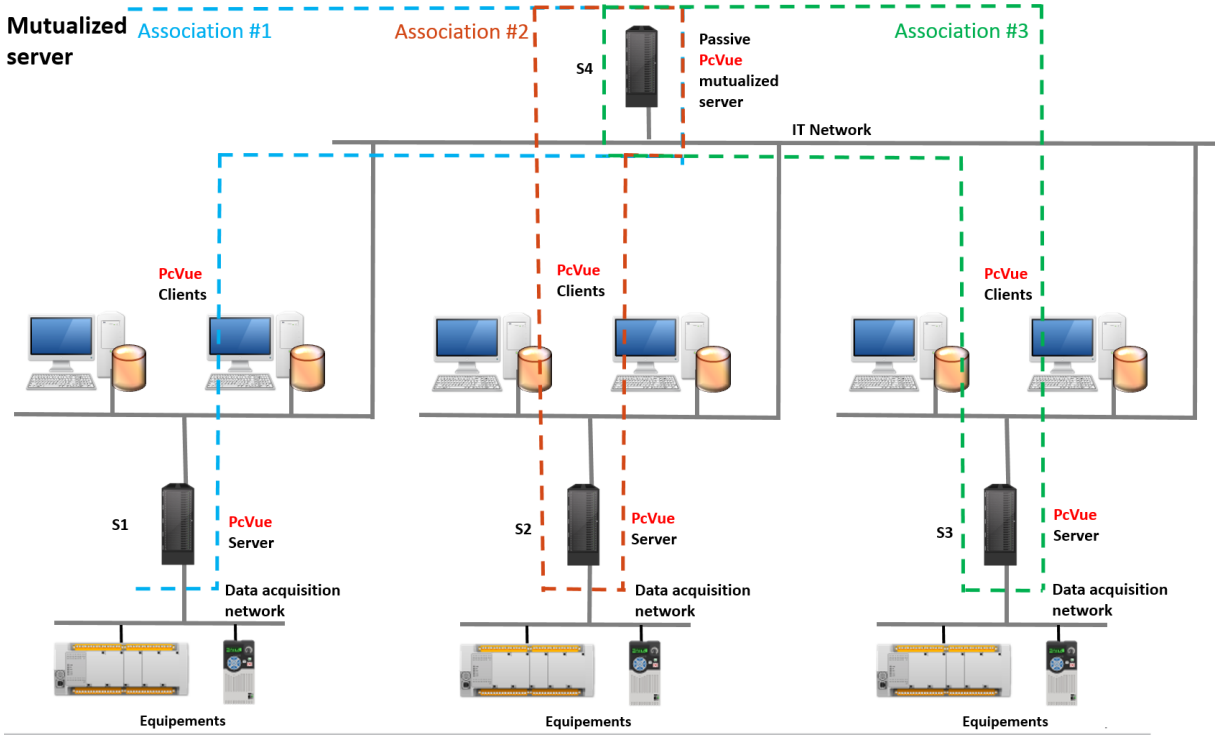
合并与标准访问（读取或写入）及通讯并行运行。
每个监控软件客户端透明地访问主动服务器的历史记录，因此可以从任何客户端站点查看连续存档的数据。

2.4.3.2 带一个数据库的模式

原理是一台机器运行管数据库和 SQL Server 引擎（最好是 Windows Server 操作系统），它与两台实时服务器 PcVue 是不一样的。
遵循先前描述的单主动服务器原理，只有主动的 PcVue 服务器将信息存储在数据库中。 因此，在所有情况下，始终至少有一个历史服务器可以存档信息。
如果数据库机器出现故障，则主动的 PcVue 服务器会在本地存储信息。 当与 SQL Server 数据库的连接恢复时，主动服务器将本地生成的存档传输到中央数据库。
只要有一台历史服务器正常运行，其集成的功能就能够确保存档的连续性。

2.5 多重冗余服务器

- ✓ 优化的冗余架构，用于监控和控制多个项目
- ✓ 减少部署和维护工作



多重冗余架构是高可用性架构的一个扩展。
当您必须监视和控制多个流程，生产线，工厂，建筑物，站点.....并且需要可靠的网络时，您可以设置一个高端服务器，该服务器将用作多个区域的备用服务器。 通过共享备用服务器，您可以实现冗余和可用性，同时最大限度地减少部署和维护完全重复服务器集群的工作量和成本。

此架构可能不能应用在任何通讯协议中，请联系技术支持以获取更多信息。

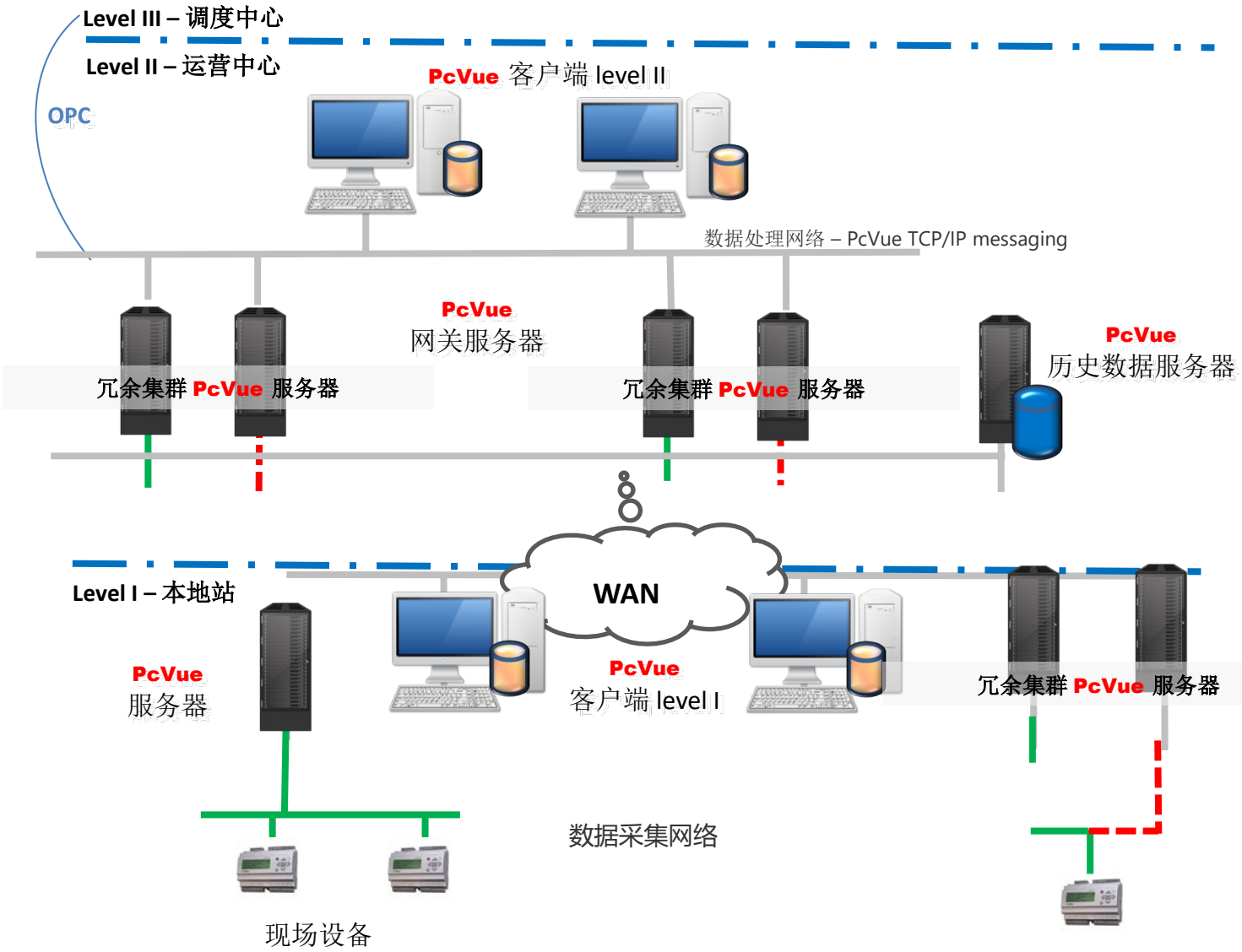
2.6 多层架构

当网络需要分段时，可以将网关添加到架构中。
例如，当系统跨广域网时，或者当数据消费者站（客户站或数据存存储）位于不太可信的网络中时，这种架构是有用的。
这样的网关可以部署在DMZ中，如果需要，网关可以是冗余的。

在分布式架构中，每个站即可以是一些变量的数据源站（生产者），又可以是另一些变量的消费者站。此外，一些站可以充当位于另一区域的中央控制室的数据集中器。
PcVue允许开发和部署多服务器/多客户端应用程序，其中部分服务器集群配置为从设备采集数据，部分服务器集群配置为从其他服务器采集数据（如客户端）。
中央服务器仅采集所有数据的子集，以便更高效地效监控设备

2.6.1 多层架构：部署#1

- ✓ 适用于超大规模应用和地理分布广泛的系统
- ✓ 不同级别控制
- ✓ 非常灵活



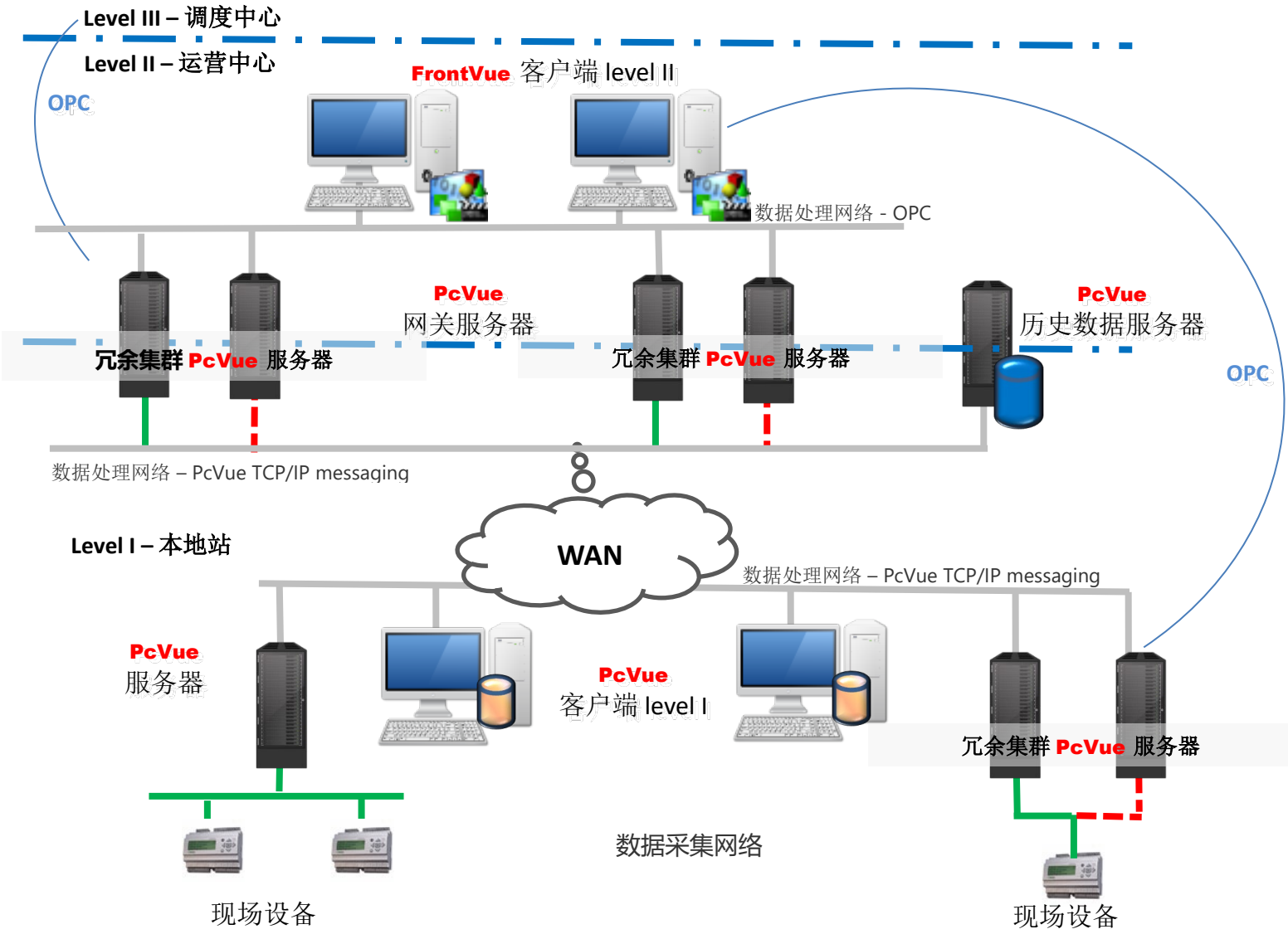
I 级 – 本地站点由广泛分布的 PcVue 站组成，从现场设备获取数据，并通过具有卫星连接的广域网将数据提供给 II 级。

II 级 – 操作中心是系统架构的核心，具有 PcVue 服务器的冗余集群，以集中来自 I 级的不同站的数据。服务器的每个集群处理数千个实时变量并在本地归档更重要的变量数据。

一对服务器也可以专用于将低级别的重要数据存档到 DBMS。
连接到服务器站的客户端站用作操作和工程控制台，并帮助操作员监视和控制来自任何站点的变量（实时，报警.....）。
III 级 - **调度中心**是该架构的最高级别。 它通过 OPC 从级别 II 统获取主要数据。

2.6.2 多层架构：部署#2

- ✓ 适用于地理分布广泛的系统
- ✓ 多个级别的控制
- ✓ 对于非常**大量的数据**/高增长率项目
- ✓ 非常灵活



当应用程序变得更大（超过 30 万个变量）时，使用更轻量级的 FrontVue HMI 客户端优化系统架构、替换全功能的 PcVue 客户端是有意义的，以确保系统的可扩展性。

FrontVue 是一个非常轻量级的基于 OPC 的 HMI 客户端，没有嵌入式处理或存档。 它作为 OPC 客户端连接到 PcVue，它可以监控和控制实时数据，并可以显示在 PcVue 端管理的报警和历史数据。

FrontVue仅刷新显示的数据以便于：

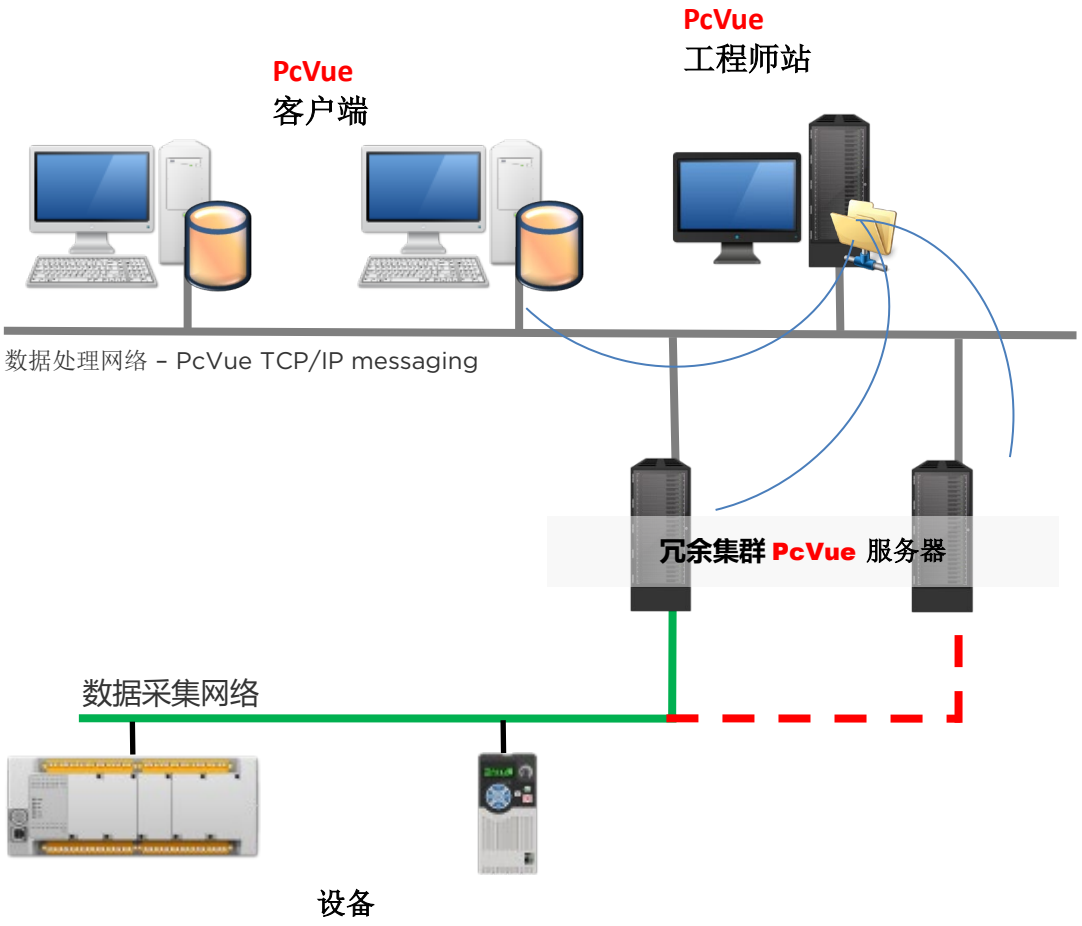
- 最大限度地减少客户端的应用程序启动时间
- 大幅减少网络上的数据负载

FrontVue可以连接多个OPC服务器以便于：

- 连接到远程本地服务器以从任何特定设备检索详细信息。
- 显示来自多个PcVue服务器的串联事件，以在警报/日志查看器中向操作员显示单个/唯一列表。

2.7 带版本管理的工程师站

- ✓ 轻松维护和部署项目和/或库
- ✓ 无限数量的版本
- ✓ 修改跟踪
- ✓ 降低错误和丢失的风险



为了使项目的维护和部署更容易、更快，PcVue 提供了**内置的中央项目管理工具**。
不同版本的项目和/或库集中在网络上的共享目录中。 可以从网络上的任何工作站加载和修改它们。
通常，专用的 PcVue 工程师站用于托管中央版本目录并对项目进行更改
任何工作站都可以手动加载和运行任何类型的版本，或者从中央项目目录自动加载和运行项目和/或库的一个参考版本。

支持的功能有:

- 3 种类型的版本：开发、操作和参考
- 版本的可配置内容
- 跟踪每个版本的修改
- 自动版本编号系统
- 无限数量的版本（磁盘空间足够大）

2.8 Web 和移动架构

本节介绍了为 PcVue 12 及更高版本部署基于 Web 和移动设备的架构的最佳方式和常见模式。

PcVue 12 在 Web 和移动组件的部署以及整合到 IT 环境中有几项改进，特别是可以将 Web 服务器层与工业网络分开。强烈建议利用这种新的职责分离功能，并在 DMZ 上与工业或 SCADA 网络隔离 Web 服务器。但是这种方案不可能在所有系统中都适用，特别是在较小规模的系统中，这就是为什么本节将重点放在各种不同的部署方案上：

- 独立一体化设置的简化方法，
- 大型企业 SCADA / HMI 系统，
- 远程访问小型系统

2.8.1 EasyMobileTechnology

PcVue 的 Web 和移动解决方案采用专有的独家技术 EasyMobileTechnology，允许设置没有网关/插件的移动架构，嵌入所有必要的安全功能（https，OAuth，证书）和 HTML5 技术以及维护工具。

该技术符合以下标准：

- 没有网关，没有额外的插件
- 无需在客户端上安装任何软件
- 简单设置 – 无脚本 – 仅限向导
- 对第三方应用程序开放
- 适应任何用户：最终用户，SI，IT
- 安全可扩展的架构和通信
- 易于诊断

2.8.2 Web 部署控制台

Web 部署控制台是用于设置、部署和维护 Web 或移动架构的组件。
它支持以下功能：
：

- ✓ 在 IIS 上部署 Web 服务和 Web 应用程序
- ✓ PcVue Web 后端端点管理
- ✓ 数据保护管理
- ✓ 证书管理
- ✓ 用户访问日志记录和 OAuth 服务器管理
- ✓ IIS 审核/诊断

Web 部署控制台运行在托管 Web 服务器 IIS 的服务器上。

2.8.3 Web 和移动客户端

2.8.3.1 HTML5 Web 客户端

WebVue 是一个使用 Web 浏览器和 Internet 或 Intranet 连接的 Web 客户端，可以远程显示和控制 PcVue 项目。 具有适当用户权限（用户名和密码）的用户可以从网络上的任何位置访问 PcVue SCADA 应用程序。 WebVue 在 Web 浏览器中运行时独立于操作系统，它直接显示 PcVue 画面，无需任何修改。
PcVue Web 服务器和 WebVue 客户端之间的通信使用 Microsoft IIS 技术和企业防火墙来管理安全性。

2.8.3.2 TouchVue – 带报警和实际推送服务功能的移动 APP 应用

TouchVue 移动应用程序允许移动设备（平板电脑，智能手机.....）通过 PcVue Web 服务器的公共 Web 服务来访问变量的实时值、不同的警报、历史列表以及曲线趋势。例如，操作员可以确认警报或强制设定点等。

2.8.4 架构 #1: 一体化部署

- ✓ 单机一体化设置的简化方法
- ✓ 安全性低
- ✓ 用于局域网且与外部访问完全隔离的情况

2.8.4.1 介绍

在此部署方案中，PcVue Web 后端站和 Web 服务器组件未分开。 它们在同一台计算机上运行。

Web 和移动客户端（包括 WebVue 和 TouchVue）连接到与 Web 服务器相同的网络。

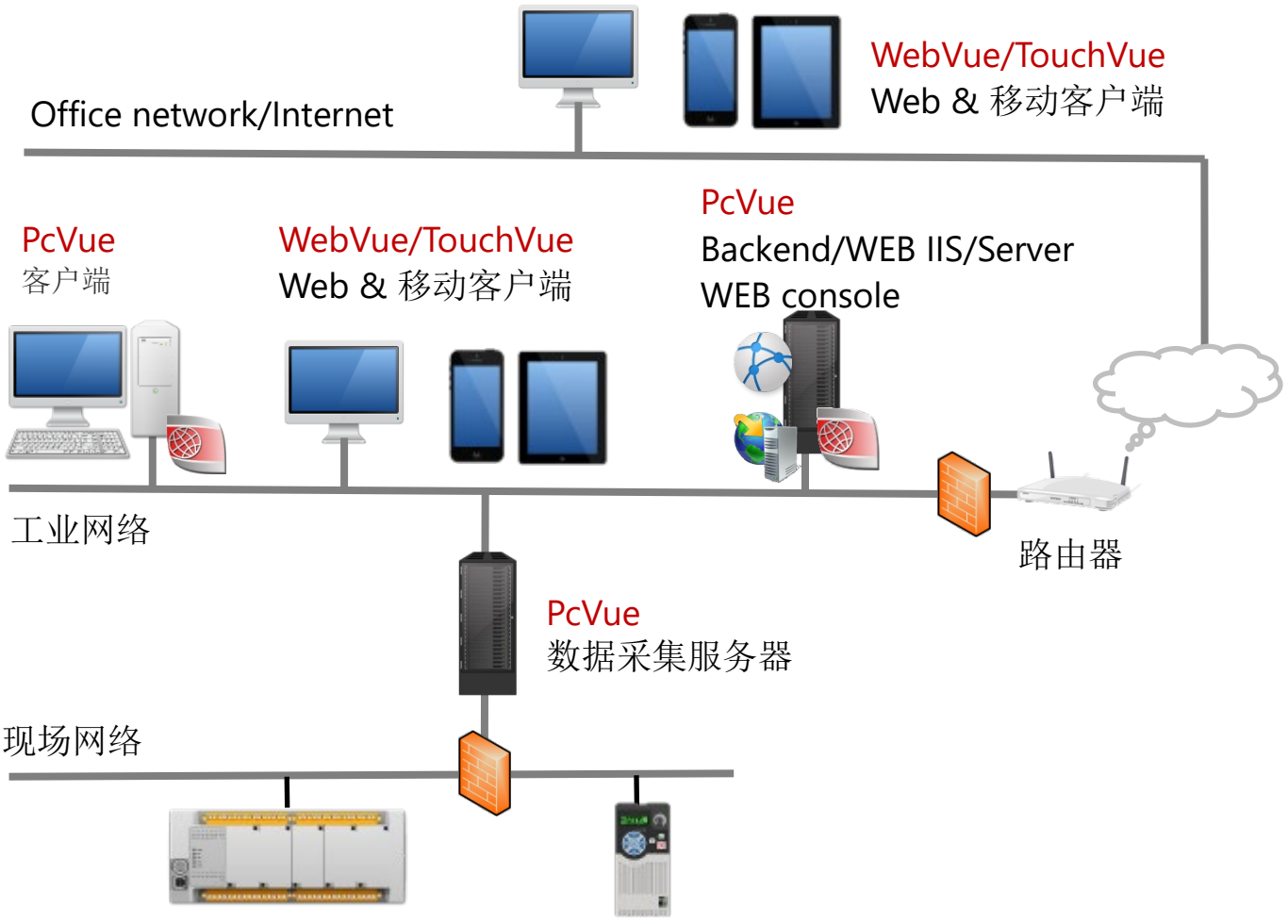


图 1 – 架构#1 – 一体化部署

注意:

- 根据 RFC 6890 中描述的典型使用模式，IP 范围和地址完全是为了说明需要，也可以使用任何其他子网范围或地址集。
- PcVue SCADA 系统的架构完全是为了说明需要，可能与您的实际设置不同。
- 尽管建议将工业网络与自动化网络分离，但完全是为了说明需要。

2.8.4.2 什么时候使用?

此架构适用于 Web 和移动客户端与 PcVue Web 后端站位于同一子网上的部署方案。

当网络（子网）是私有的，并且与外部访问完全隔离时，此部署方案的使用相当适合。 特别是操作人员使用的计算机和设备也不得访问外部网络，以避免被用做访问工业网络的入口。

2.8.4.3 什么时候不适用?

当网络对来自外部网络的传入请求开放或打开来自未知设备的不受保护的访问时，请勿使用此方案。

特别是当需要从 Internet 上的 Web 和移动客户端系统进行访问时，不要使用此方案，也不建议使用其他网络安全手段（例如 VPN 隧道）。

2.8.4.4 要求

1. 此架构的部署需要最低水平的网络专业知识。
2. 要求所有计算机和移动设备位于同一子网上，通常是工业网络，包括 Web 和移动客户端，Web 服务器和 PcVue Web 后端站。
3. 此网络上的客户端应该毫无保留地信任 Web 服务器计算机，因为它们位于同一个网络上，并且根据定义，它是私有网络。
4. 此架构对 Web 服务器证书的可信赖性的最低要求起作用。来自证书颁发机构的证书不是强制与 Web 服务器建立信任的证书。

2.8.4.5 优势

1. 只需要一台计算机来托管 PcVue Web 后端和 Web 服务器。
2. 此计算机不需要多个网卡。

3. Web 和移动客户端直接使用 Web 服务器计算机的 IP 地址连接即可访问。

   Windows 平台上的域名解析不需要 DNS。 Web 服务器计算机可以通过其主机名从任何基于 Windows 的 Web 客户端进行寻址。

   如果为有限数量的用户提供服务，则可以在 PcVue Web Server 计算机上使用 Windows 桌面操作系统（如 Windows 10）。在所有情况下，强烈建议使用服务器操作系统。
   使用非 Windows 客户端设备（Android，iOS，Linux）时，DNS 服务器的存在是名称解析的必要条件。这可以通过使用用于 PcVue Web 后端站的 Windows Server 操作系统和激活 DNS 服务器角色来实现。

4. 自签名证书的使用是开箱即用的，但需要在 Web 客户端中添加安全例外，或者在移动客户端应用程序上启用“忽略证书错误”选项。

   如果有可从网络访问的 Active Directory 服务器，则可以从 Active Directory 服务器颁发域证书，并由域的所有客户端（通过域策略或通过公司 MDM 系统）信任。

2.8.4.6 限制

1. 在 Windows 桌面操作系统上托管 Web 服务器时会有限制。 特别是 IIS 可以处理的最大客户端连接数是有限的。

2. 如果主机名不是 FQDN，Microsoft®Edge 不允许存储 cookie。 这会导致 Web 组件出现问题。 可以通过将 URL 更改为：

   https://<hostname>.local

3. 当使用无效（部分受信任或不受信任）证书时，可能会遇到有限的性能，特别是在 WebVue 客户端加载期间，因为在这种情况下，文件不会被 Web 浏览器缓存。

2.8.4.7 Web 部署控制台

可以使用 WDC 的“快速设置”向导将所有设置保留为其默认值，来轻松部署此架构。因此，WDC 需要与 PcVue Web 后端和 Web 服务器安装在同一台计算机上。

2.8.5 架构#2: 网络隔离和 DMZ

- ✓ 大型企业 SCADA / HMI 系统
- ✓ 高水平的安全性
- ✓ 当 Web /移动客户端位于工业网络之外时

2.8.5.1 Description 介绍

在此架构中，PcVue Web 后端站与 Web 和移动客户端位于不同的物理或逻辑网络上，处于不同的安全范围，需要与 DMZ 隔离。 内部网络（DMZ 路由器的 LAN 侧）是专用安全网络。 外部网络（DMZ 路由器的 WAN 侧）是不太受信任的网络，通常是公司办公室网络或 Internet。

Web 服务器组件托管在 DMZ 内的计算机上，PcVue 后端托管在安全网络上。

该架构提供了与 IT 网络的最佳集成，并允许最大程度地遵守 IT 指南和实践。

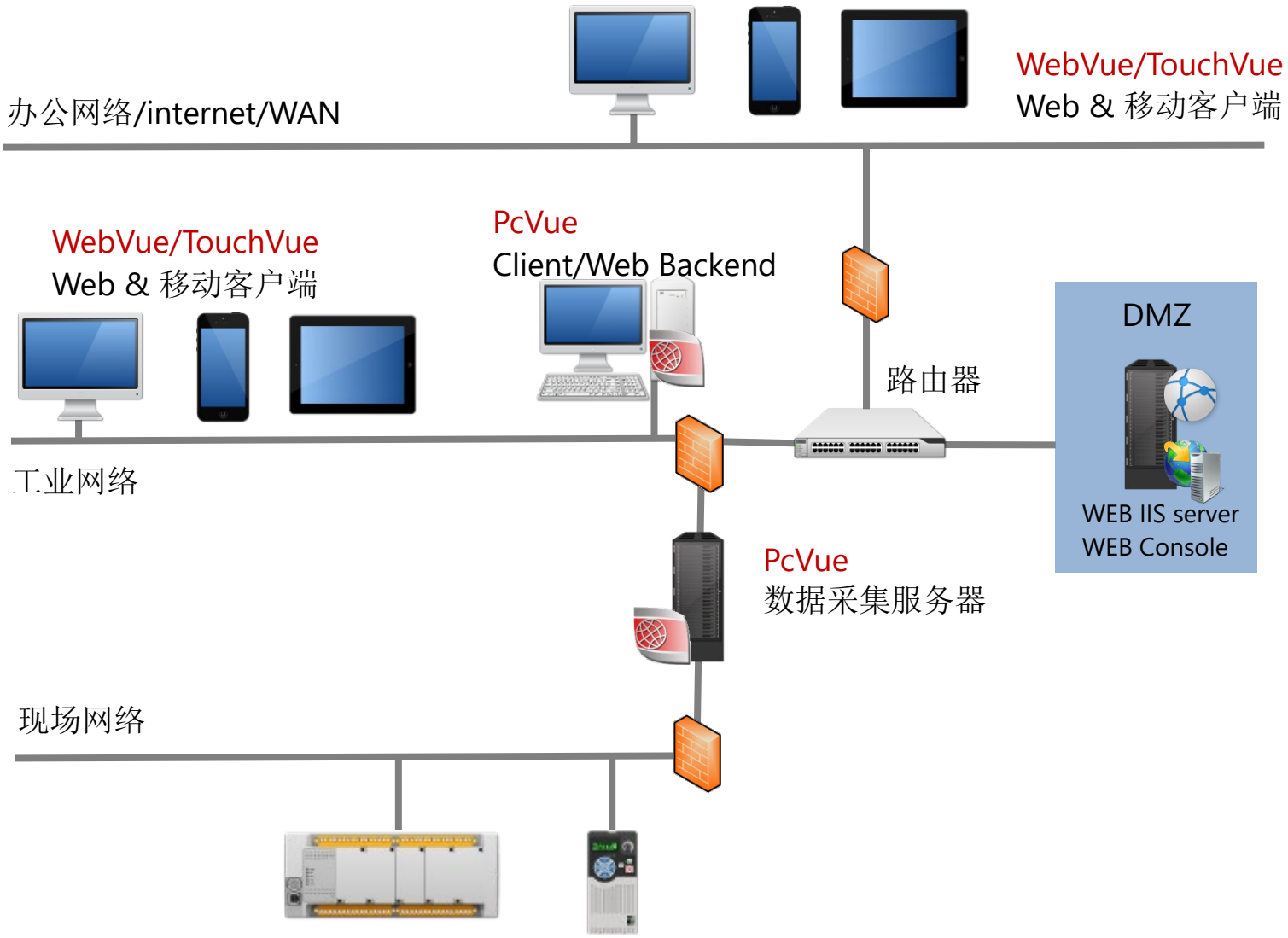


图 2 – 架构#2 – 网络隔离和 DMZ

注意:

- 根据 RFC 6890 中描述的典型使用模式，IP 范围和地址完全是为了说明需要，也可以使用任何其他子网范围或地址集。
- PcVue SCADA 系统的架构完全是为了说明需要，可能与您的实际设置不同。
- 尽管建议将工业网络与自动化网络分离，但完全是为了说明需要。

2.8.5.2 什么时候使用?

只要 Web 和移动客户端不在安全的工业网络上，就建议使用此部署架构。

2.8.5.3 要求

1. 部署此架构所需的网络和 IT 专业知识水平从中级到高级。

2. 需要合适的网络架构来将专用网络与受保护较少的网络隔离开来。 这包括路由器（以及足够的路由配置）和至少一个防火墙。

   支持常见的 DMZ 架构，包括单防火墙设置和双防火墙设置：

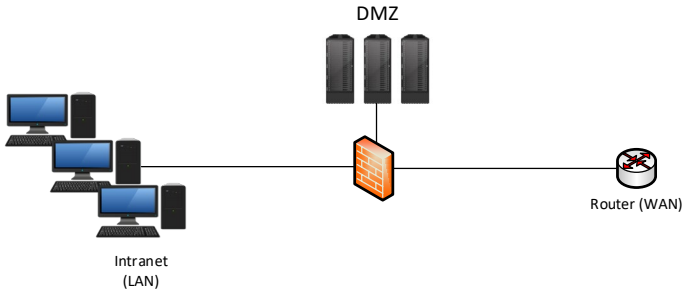


图 3 - DMZ – 单防火墙设置

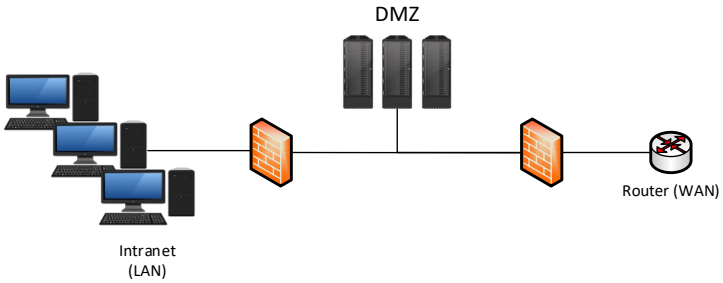


图 4 - DMZ – 双防火墙设置

3. 可能需要得到最终用户的 IT 部门支持才能正确设置网络隔离、名称解析和证书。

   这包括正确的配置：
   - DNS
   - 路由
   - NAT（或端口转发）
   - 证书

   作为公司 PKI，可能需要 Active Directory 基础结构来颁发证书并确保信任关系作为全局策略的一部分。

4. 为了验证较小的可信网络上的 Web 服务器计算机的身份并防止中间人攻击，必须使用完全受信任的证书。

   - 此证书可由 IT 部门（公司网络 Active Directory 服务器）颁发。如果所有 Web 和移动客户端都与企业网络架构处于可信关系，那就足够了。

   - 此证书可由 IT 部门通过可信 CA 颁发。如果 Web 服务器是由外部 Web 和移动客户端访问的必要条件（客户端设备/计算机与公司网络基础架构不存在信任关系的典型访问）。

   - 如果存在 Internet 访问，且用户组织策略允许 Let's Encrypt®服务，则可以通过 WDC 的 Let's Encrypt®向导发出此证书。

5. 较小的可信网络上需要能够解析 Web 服务器名称的 DNS 服务器。

6. Web 服务器计算机上的 Windows Server 操作系统，理想情况下也位于 PcVue Web 后端站上。
7. 必须至少通过其 IP 地址访问 Web 服务器计算机上的 PcVue Web 后端站。由于 DMZ 内存在名称解析的平均值，因此也可以通过主机名进行访问：
   - Web 服务器计算机的 hosts 文件中的专用条目。
   - 工业网络中可从 DMZ 访问的 DNS 服务器。

   如果尚未提供，则可以在 PcVue Web 后端站的 Windows Server 操作系统上激活 DNS 服务器角色。

   注意：允许从 DMZ 内的计算机访问专用网络与 DMZ 常见模式和实践相矛盾。但是，由于技术原因，需要向该端口打开 TCP 端口 8090。

2.8.5.4 优势

1. 通过在完全合格的域名下公开 Web 服务器的 Web 和移动服务以及应用程序，该架构允许从不太可信的网络（通常是 Internet 或 Intranet）方便地访问。
2. 它允许根据 IT 网络隔离做法对网络流量进行最大程度的控制，确保从外部网络到工业网络不存在不期望的传入连接请求，包括网络周边的流量控制和监控。

2.8.5.5 Web 部署控制台

可以使用任何 WDC 设置向导来部署此架构。 “快速设置”向导的默认设置并不适用于所有情况。WDC 需要安装在 Web 服务器计算机上。

2.8.6 架构#3: 用于远程访问的简化 NAT 方案

- ✓ 远程访问小型系统
- ✓ 在没有可用的托管 IT 架构时使用

2.8.6.1 Description 介绍

此部署方案对应于单个专用 LAN，即工业网络，其中 Web 服务器，PcVue Web 后端站和大多数 Web 和移动客户端都驻留在其中。专用 Internet 访问用于远程连接。
在此部署方案中，Web 和移动客户端分布在 NAT 边界（本地和远程 Web 客户端）的两侧。

虽然这样部署此架构在技术上是可行的，但不建议在不部署其他安全措施的情况下这样做。

可行的方案包括 VPN 的使用和客户端地址锁定，在这种情况下，架构可能在逻辑上等于架构＃1。通过使用网络边界的专用 DMZ 端口来建立专用网段，在这种情况下，架构是架构＃2 的简化版本。在任何情况下，建议将 PcVue Web 后端站和 Web 服务器分开，如架构＃2 中所述，这本身就是一种额外的安全措施。
如果通过第三方提供 Internet 访问并且需要由 ISP 提供和操作的机顶盒等设备，则强烈建议安装用于控制网络边界的设备。特别提醒，强烈建议不要使用替代解决方案，例如“暴露主机”模式。

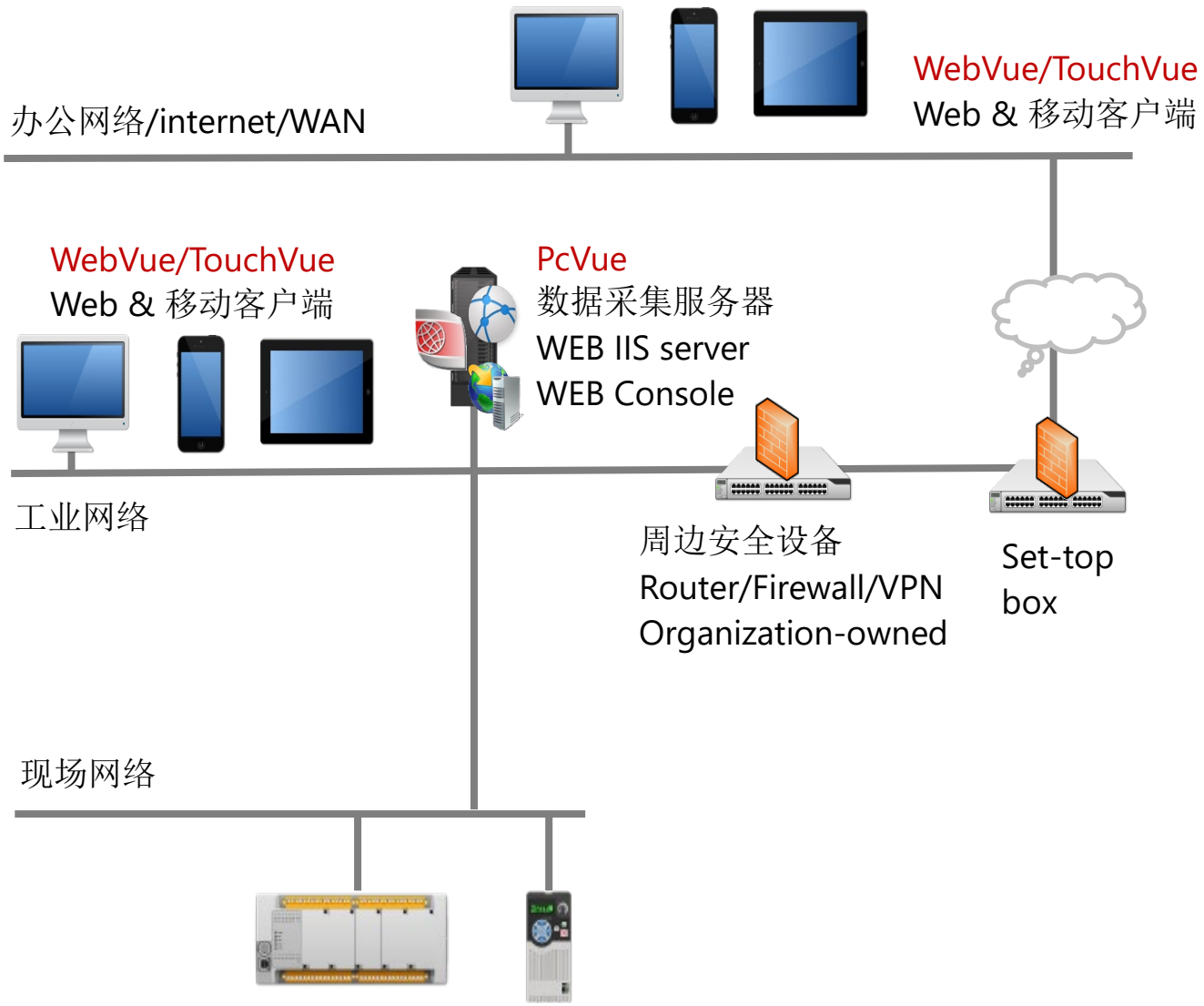


图 5 – 架构 #3 – 用于远程访问的简化 NAT 方案

注意:

- 根据 RFC 6890 中描述的典型使用模式，IP 范围和地址完全是为了说明需要，也可以使用任何其他子网范围或地址集。
- PcVue SCADA 系统的架构完全是为了说明需要，可能与您的实际设置不同。
- 路由器设备暴露给 WAN 的 IP 地址可能取决于您的 ISP。
-

2.8.6.2 什么时候使用?

当没有可用的托管 IT 基础架构时，可能需要此部署方案进行简单的远程访问。

我们建议使用此类架构运行旧版 WebVue 的现有系统迁移到架构＃2 或应用其他安全措施。

2.8.6.3 什么时候不使用?

如果不了解与不良网络隔离和弱网络流量控制相关的风险，请不要在生产环境或现实系统中使用此架构。

2.8.6.4 要求

1. 部署此架构所需的网络和 IT 专业知识水平低至中等。

2. 用于在专用网络和受保护较少的网络之间建立连接的网络结构。用于连接路由器任一侧的 Web / 移动客户端的网络结构。

3. 在网络边界上配置的网络地址转换（或特定端口转发）。

4. 为了验证较小的可信网络上的 Web 服务器计算机的身份，并防止中间人攻击，必须使用完全受信任的证书。

   - 此证书可由 IT 部门通过可信 CA 颁发。如果 Web 服务器是由外部 Web 和移动客户端访问时必须要有（客户端设备/计算机与公司网络基础架构不存在信任关系的典型访问）。

   - 如果存在 Internet 访问，且用户组织策略允许 Let's Encrypt®服务，则可以通过 WDC 的 Let's Encrypt®向导颁发此证书。

5. Web Server 和计算机必须可以从两个网段访问 Web Server 计算机。

   如果 Web 服务器在同一 FQDN 下的两个网段上都是众所周知的，则可以实现这一点。

   如果不是这种情况，则需要 Web 和移动客户端通过使用其 FQDN 直接连接到 Web 服务器计算机而不必使消息必须离开专用网络。在这种情况下，建议使用 NAT Loopback / Hairpinning。

如果这些选项都不可能满足，建议通过 WDC 创建两个不同的站点，这两个站点都连接到同一个 PcVue Web 后端站

2.8.6.5 优势

1. 该架构允许方便地访问位于工业网络和 Internet 上的 Web 和移动客户端。
2. 此架构是提供远程 Web 访问的老 WebVue 系统迁移过程的第一步。

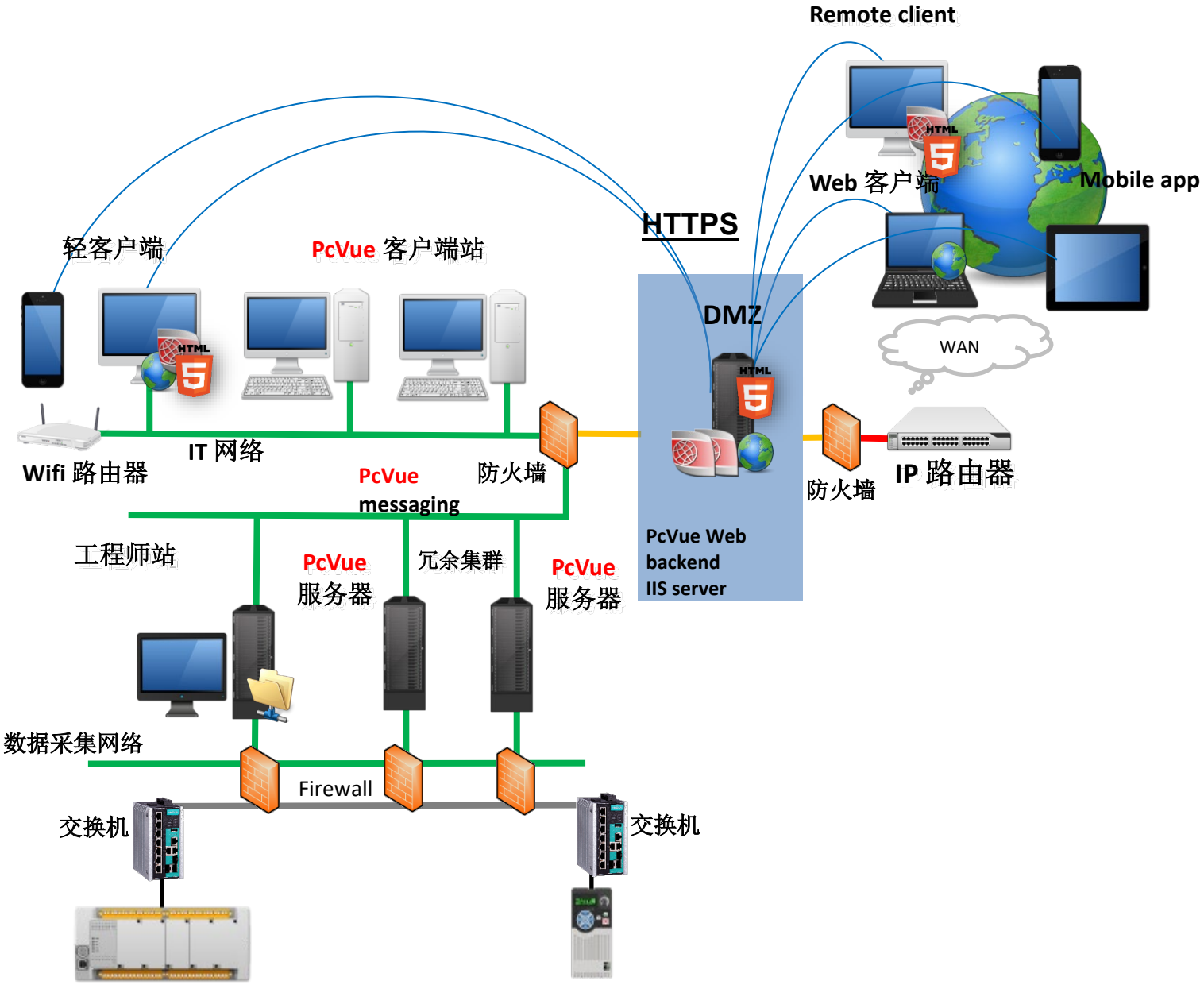
2.8.6.6 限制

如果未添加特定设备来控制网络边界，则此部署方案提供有限的网络安全性，因为：
- 您依靠 ISP 拥有的机顶盒来控制网络边界和远程连接，
- 作为工业控制系统一部分的计算机直接暴露于互联网。

在最糟糕的情况下，攻击者可利用多个级别上的潜在安全漏洞来访问工业控制系统。

2.8.6.7 Web 部署控制台

可以使用任何 WDC 设置向导来部署此架构。WDC 需要安装在 Web 服务器计算机上。



2.9 混合架构

此架构的示例取决于下面的元素：

- 数据采集由工业网络上的冗余采集服务器执行。
- 开发站用于项目的集中管理。
- 操作在客户端站上执行，客户端位于防火墙隔离的计算机网络上.

- 安装在防火墙隔离的控制区（DMZ）中的 Windows 服务器上的工作站，托管 Web 服务器，移动服务器和 Windows RDS 服务器。
- 可以使用 Windows 远程访问组件通过 RDS 实例远程运行客户端。
- 安装在服务器上的接口允许在支持 HTML5 的任何设备上显示客户端实例。
- Web 客户端允许从标准 Web 浏览器进行操作。
- 连接到移动服务器的移动应用程序用于通过智能手机或平板电脑通知和确认警报和控制。
- Web 服务器和终端之间的交换使用安全套接字 HTTPS。
- Windows Active Directory 管理整个系统的用户访问，以进行单点登录（SSO）

必须采取一些预防措施来保护PcVue多层架构的组件。

所以必须：

- 通过创建需要相同安全级别的VLAN来划分各种网络（例如计算机和工业）

- 使用防火墙过滤数据。

使用DMZ和路由器还允许将网络与外部隔离并防止不必要的入侵。

为了保护两个网络组件之间的通讯流量，也可能需要建立VPN隧道解决方案。 通常，可以在PcVue采集站和通过TCP / IP通信的PLC之间建立VPN，或者在与多个远程监控站点之间建立VPN。

PcVue Solutions与MOXA合作，提供完整的硬件保护解决方案，以解决上述问题：

-全系列安全的工业防火墙/ VPN
- 不同网络区域之间的流量限制和控制
- 创建流量限制

2.10 虚拟化

- ✓ 减少物理站的数量
- ✓ 减少管理工作量和成本
- ✓ 低成本的瘦客户端
- ✓ 在瘦客户端上免费安装
- ✓ 符合 IT 要求

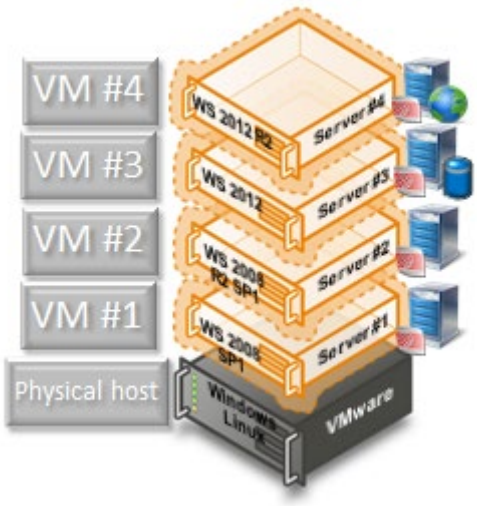
虚拟化在计算中是指创建某物的虚拟（而非实际）版本的行为，包括但不限于虚拟计算机硬件平台，操作系统（OS），存储设备或计算机网络资源。

硬件虚拟化或平台虚拟化是指创建一个虚拟机，其功能类似于具有操作系统的真实计算机。 在这些虚拟机上执行的软件与底层硬件资源分离。
在硬件虚拟化中，主机是发生虚拟化的实际机器，而客户机是虚拟机。 单词“host”和“guest”用于区分在物理机器上运行的软件与在虚拟机上运行的软件。
工业应用程序的虚拟化可以使许多相关部门受益：IT、工程和运营。

2.10.1 应用虚拟化

✓ VMWare 主机可以在隔离环境中运行不同版本的 PcVue 或 FrontVue
✓为一次性操作设置工作环境变得容易
✓可以建立一个老的操作系统
✓在 Windows 7，Windows 8，Windows 8.1，Windows 2008 SP2 和 2008 R2 SP1,2012 和 2012 R2 Server 和 VMWare 下运行

2.10.2 资源虚拟化

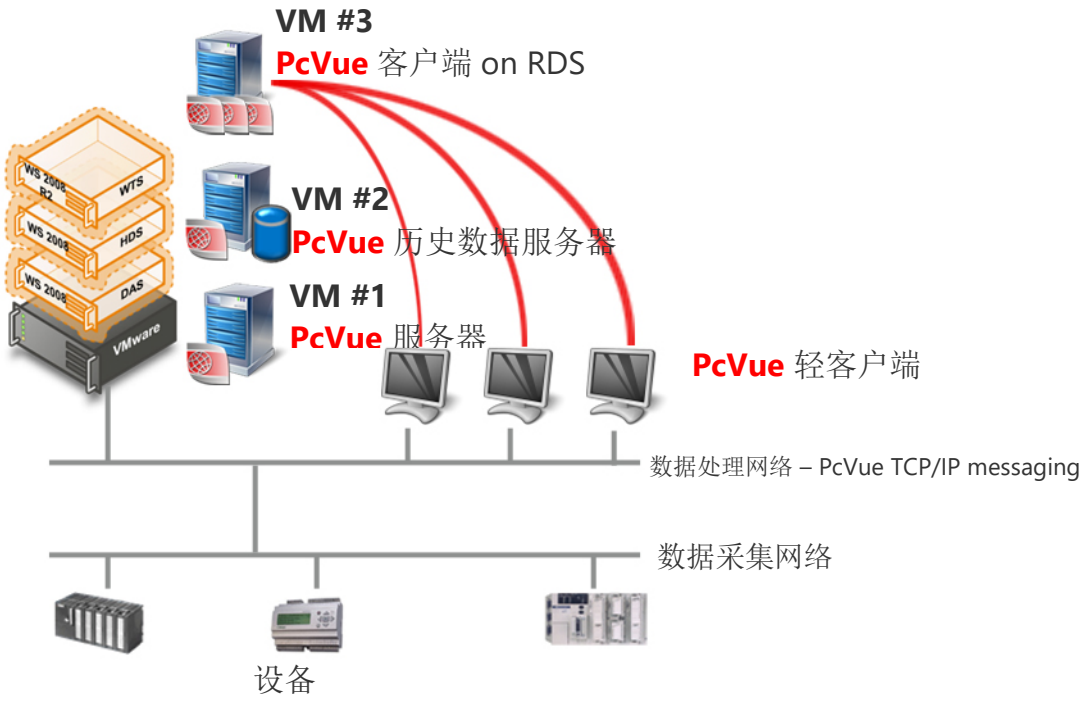


✓虚拟化环境可以在单个物理机器上的不同操作系统下运行各种PcVue服务器

✓PcVue许可证可以是不同类型的

✓根据资源优化规则将虚拟机动态分配给物理主机

2.10.3 部署示例



SCADA应用程序在IT管理站上运行。 运行VMware的单个物理机器或同等主机托管隔离虚拟机中的所有站，其中一个VM运行RDS，允许多个RDS客户端站连接到服务器。 本文中描述的大多数架构都可以部署在虚拟环境中。

3. 专有词汇

名称	缩写	介绍
Microsoft® Internet Information Services	IIS	Internet 信息服务（IIS）是由 Microsoft®创建并随 Windows 操作系统一起提供的 Web 服务器。 IIS 是 Microsoft®Windows 操作系统上的内置 Web 服务器。
PcVue Web back end station		工业网络上的 PcVue 站用作 PcVue 多站系统和实际 Web 服务器（IIS）之间的网关。 Web 后端运行 Sv32.exe，即 PcVue 主进程。
Web Server machine Web Server computer		运行 IIS Web 服务器的计算机，该计算机又托管 PcVue Web 服务器组件。 Web 服务器不运行 Sv32.exe（PcVue 主进程本身）.
PcVue Web Server Components		在 Web 服务器计算机上安装的一组服务和应用程序，用于连接 PcVue 的 Web 和移动客户端。
Web & Mobile Client Systems		在智能移动设备上在 Web 浏览器或本机移动应用程序（如 TouchVue）中运行 WebVue Web 客户端的计算机和设备。
Web Deployment Console	WDC	安装在 Web 服务器计算机上的桌面应用程序，允许系统管理员配置、部署和监视 IIS 和 PcVue Web 服务器组件。
Industrial Network		包含 PcVue SCADA 网络的网段。 在 ANSI / ISA-95 信息模型（也称为 SCADA 级别）中称为 2 级工业网络
Demilitarized Zone	DMZ	DMZ 或非军事区 - 有时称为外围网络 - 是一个物理或逻辑网络，它包含并向组织的不受信任的网络（通常是更大的网络，如 Internet）公开面向外部的服务。 DMZ 的目的是为组织的局域网（LAN）添加额外的安全层。
Fullly Qualified Domain Name	FQDN	一个域名，指定其在域名系统（DNS）的树层次结构中的确切位置。它指定所有域级别，包括至少一个二级域和一个顶级域。
Domain Name System	DNS	DNS 是用于连接到 Internet 或专用网络的计算机、服务或其他资源的分层分散命名系统。
Windows Internet Name Service	WINS	WINS 是 Microsoft®的 NetBIOS 名称服务（NBNS）的实现，它是 NetBIOS 计算机名称的名称服务器和服务。
Subnetwork	Subnet	子网是 IP 网络的逻辑细分。 属于子网的计算机在其 IP 地址中使用通用、相同、最重要的位组进行寻址。 当源地址和目标地址的路由前缀不同时，通过路由器在子网之间交换流量。 路由器充当子网之间的逻辑或物理边界。
Virtual Private Network	VPN	虚拟专用网络（VPN）通过公共网络扩展专用网络，并使用户能够跨共享或公共网络发送和接收数据，就好像他们的计算设备直接连接到专用网络一样。
Firewall		它是一个网络安全系统，它根据预定的安全规则监视和控制传入和传出的网络流量。
Network Address Translation	NAT	NAT 是一种通过修改数据包的 IP 报头中的网络地址信息将一个 IP 地址空间重新映射到另一个 IP 地址空间的方法，同时它们通过流量路由设备传输。 NAT 网关的一个可联网路由的 IP 地址可用于整个专用网络。

名称	缩写	介绍
Port Forwarding	PAT	端口转发或端口映射是网络地址转换（NAT）的应用程序，当数据包穿过网络网关（例如路由器或防火墙）时，它将通信请求从一个地址和端口号组合重定向到另一个。 此技术最常用于通过将通信的目标 IP 地址和端口号重新映射到驻留在网关（外部网络）另一侧的主机上的受保护或伪装（内部）网络上的主机上进行服务。
Internet Service Provider	ISP	Internet 服务提供商（ISP）是一种提供访问，使用或参与 Internet 的服务的组织。
Private Key Infrastructure	PKI	公钥基础结构（PKI）是创建、管理、分发、使用、存储和撤销数字证书以及管理公钥加密所需的一组角色、策略和过程。
Certificate Authority	CA	证书颁发机构或证书颁发机构（CA）是颁发数字证书的实体。 CA 可以是受信任的第三方，也可以是公司 PKI 的一部分。
Mobile Device Management	MDM	移动设备管理是移动设备管理的行业术语，例如智能手机，平板电脑，笔记本电脑和台式电脑。 MDM 主要处理企业数据隔离，保护电子邮件，保护设备上的公司文档，实施公司策略，集成和管理移动设备。
Hypertext Transfer Protocol Secure Hypertext Transfer Protocol	HTTP / HTTPS	超文本传输协议（HTTP）是用于分布式，协作式和超媒体信息系统的应用程序协议。 HTTP 是万维网数据通信的基础。 HTTPS（安全的 HTTP）是用于安全通信的超文本传输协议（HTTP）的扩展。 该协议通常称为 HTTP over TLS 或 HTTP over SSL。
Hairpinning		Hairpinning（也称为“NAT 环回”）描述了使用其映射端点在同一 NAT 设备后面的两个主机之间的通信。 Hairpinning 是 LAN 上的机器能够通过 LAN /路由器的外部 IP 地址访问 LAN 上的另一台机器（在路由器上设置端口转发以将请求定向到 LAN 上的适当机器）。
WebSocket(s)		WebSocket（RFC 6455）是一种计算机通信协议，通过单个 TCP 连接提供全双工通信通道。 WebSocket 旨在通过 HTTP 端口 80 和 443 工作，以及支持 HTTP 代理和中介。 HTTP WebSocket 通过其 wss 绑定（Web Socket Secure）支持加密。
HTTP/2 - SPDY protocol		HTTP / 2 是 HTTP 网络协议的主要修订版。 它源于早期的实验性 SPDY 协议。 协议演进所带来的主要改进通过引入减少的延迟、报头压缩、TCP 多路复用和请求流水线来关注网站的响应性。

一些通用定义来自维基百科。无法保证准确性或适用性。

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 架构和部署