上海纽约大学苹果设备管理思路

文 / 常潘

上海纽约大学拥有相当数量的 Apple 台式机、笔记本和平板，使用场景包括：教职工的办公电脑（MacBook）、教室内用于教学的 Mac Mini 台式机、计算机机房中的台式一体机（iMac）、会议室里用于电子白板演示的平板（iPad Pro）、为师生提供免费借用服务的笔记本（MacBook）和平板（iPad Mini）。这些设备对学校的教学、科研和管理起到了非常重要的支撑作用。鉴于 Apple 系统特有的生态圈，如何集中、安全、高效地管理这些设备是一个大的挑战。

管理系统选择

Windows 系统可以通过镜像操作实现对大量设备的系统安装、软件分发和更新管理，上海纽约大学通过 LANDesk 管理系统实现了对 Windows 桌面终端的统一管理。由于 T 系列芯片在 Mac 电脑中的广泛使用，Apple 限制了 Mac 电脑的外部启动，使得适用于 Windows 系统的批量镜像操作模式在 Apple 设备的管理中几乎无法实现。

Apple 的 iOS 设备（iPad 和 iPhone）要求其软件（下文称之为 App）必须使用 App Store 安装和管理，这使得对 iOS 设备的批量软件分发几乎不可能实现。另外，Apple Mac 系统版本和软件更新会不时带来大的变化，很多设备管理系统都无法快速适应这些变化。

通过多轮的测试和对比，学校最终选择了 Jamf Pro（以下简称 Jamf）管理系统，Jamf 能管理所有系统为 macOS、iOS、iPadOS 和 tvOS 的设备，并且同时支持这些系统新老版本。Jamf 相较于其他同类系统，不仅可以提供 Apple 设备全生命周期的自动化管理，还可根据用户的个性化需求配置 Apple 设备，同时保留 Apple 设备的使用体验。从管理角度看，Jamf 的优势主要体现在如下几点。

操作便利性。Jamf 系统基于 Web 界面，对管理客户端无任何要求。

设备批量管理。设备的批量管理包括：软件和配置文件（Configuration Profile）的批量分发、操作系统及软件的版本管理。在软件分发中，Jamf 不仅能为 macOS 提供 pkg 软件的批量分发，还能实现 iOS 系统中基于 App Store 的 App 批量分发。

Syslog。Jamf 提供完整的日志记录和输出，学校通过 Splunk 收集这些日志，能够审计系统管理员的任何操作行为，对其中的敏感操作实时报警。

自助服务平台。Jamf 在被管理的客户端设备中提供了自助服务平台入口，在该平台中不仅可以发布软件安装和更新，还可以提供点对点精准支持服务。

可扩展的编程接口。Jamf 提供了完善的 REST API，通过 API 可以实现快捷条目创建、查询、更新和删除，结果可用 XML 或 JSON 格式返回。学校通过系统 API 实现了 Jamf 与资产管理系统和 IT 设备借还系统的集成：在资产管理系统中可以实时查看各 Apple 设备的使用人及使用状态信息；在借还系统中可以对 Apple 设备进行实时注册、激活与数据删除。

高活跃的 Apple IT 社区。Jamf 提供了全球 Apple IT 社区 Jamf Nation。社区中有大量活跃的、从事 Apple 设备管理和开发的资深用户。发布的问题能够及时得到解决办法，有时还会有解决方案优化建议。

Jamf 组件及系统架构

组件

Jamf 管理系统主要由 Jamf Server、Jamf Binary 和 MDM（Mobile Device Management）组成。Jamf Server 包括前端的 Web 服务器和后端的 MySQL 数据库，Web 主要提供面向管理人员的图形化操作界面、为被管理设备提供连接服务，数据库中存储所有配置和设备信息。Jamf Binary 部署在 macOS 终端中，主要用于 macOS 终端设备的信息采集和策略执行。MDM 通过将配置文件部署于 macOS 或 iOS 终端中，使得 Jamf 可以通过 Apple 消息推送（Apple Push Notification，APN）服务向被管理设备发送管理指令和部署配置文件。

系统架构和部署

系统架构和部署以稳定性和安全性为主要考虑因素，Jamf 系统架构及部署如图 1 所示。前端的 Web 服务和后端的数据库服务分开部署，Web 服务使用 Jamf 原生的冗余配置提供高可用性，数据库服务使用 MySQL 的主从架构提供数据冗余和缓解读写压力。在每台虚拟机的南北向和东西向分别设置安全策略，以白名单的方式开放所需端口并进行应用流量检查和过滤。被管理设备可以从校内或互联网连接 Jamf 服务器，通过智能 DNS 系统使从互联网连接的设备需要经过阿里云盾的过滤。Jamf 的管理员认证通过校内 SSO 实现，服务器的管理和运维必须经过堡垒机（Jump Server）。

应用场景

为便于 Apple 设备的管理，学校还使用了 Apple 校园管理（Apple School

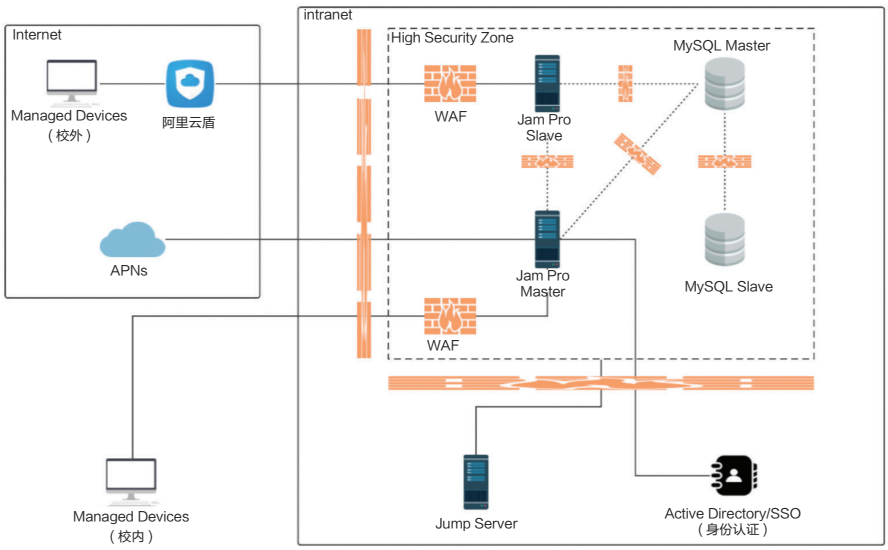

图 1 Jamf 系统架构及部署

Manager，ASM）配合 Jamf 系统，ASM 包含了 Apple 设备自动注册方案（Device Enrolment Program，DEP）和 App 批量购买计划（Volume Purchase Program，VPP）。

为了让 Apple 设备能通过 DEP 自动注册到 Jamf 中，管理员需要将设备供应商编码加入 ASM 的供应商列表中，由设备供应商完成设备信息的提交，实现 MDM 服务器的自动指派。VPP 是基于 App Store 的 App 批量购买方式，购买后的 App 可以通过 Jamf 批量安装。DEP 和 VPP 为实现从设备采购开始的全生命周期管理提供了基础。

台式机管理

学校在完成 Apple 设备的采购流程后，供应商会将订单中到货的 Apple 设备提交到 Apple 网站以注册 ASM，注册好的设备将会添加到学校的 ASM 设备列表，并自动完成 Jamf 服务地址的分配。当这些新设备开始连接互联网时，Jamf 服务将向设备自动分配自定义的预注册（pre-stage enrollment）配置，对不同用途的电脑，例如教职工电脑、教室电脑、机房电脑，学校使用不同的预注册配置。

以教职工电脑为例，在预注册配置中尽可能减少用户在 macOS 设置中的交互，并将系统的默认管理员账户设定为电脑所有者。当用户完成设置进入系统后，根据 Jamf 中的配置策略安装相应的标准软件，同时使用 DEP 通知展示正在安装软件的详细信息，包括软件名称和安装进度。

学校所有的电子设备都由信息技术部集中、统一管理，因此所有新采购的电脑都会经过 IT 的预配置后才会发放给用户。在使用 Jamf 之前，新电脑首次配置需要 IT 工程师手动完成，采用了 Jamf 和 ASM 后，通过标准化和自动化配置可以消除首次配置时的人为失误。在更换电脑所有人时，系统还能实现自动数据清除和新用户的自助配置。

笔记本和平板借还的配置与管理

学校 IT 为师生提供笔记本和平板的免费借用服务，在使用 Jamf 之前，IT 设备借还系统中的约束无法在设备管理中实施，使得资产盘点和设备找回存在困难。在采用 Jamf 后，学校将其与 IT 设备借还系统进行了集成，实现了设备必须经过借还系统验证才可使用，具体如下：

1. 用户在借还系统中通过读取校园卡和扫描设备二维码开始借用。

2. 借还系统通过 Jamf 提供的 API 向 Jamf 发送处理请求，Jamf 根据请求将被借用设备的扩展属性（Extended Attribute）的值写为 Loaned，同时将设备加入借出设备的 smart group 中。

3. 用户获得一个经过初始化的设备，根据设备的设置助理提示使用身份凭证联网并激活设备。

4. 设备在激活后，会根据 AppleAPN 云服务自动下发的 MDM Profile 进行配置，并加入 Jamf 的管理池中。

5. 设备根据上述 Loaned smart group 中的策略来自动完成软件的安装和策略的设定。

为确保用户数据的安全，每一台借用并归还的 iPad 设备，都会进行数据抹除。IT 通过多种不同的方式在归还前提示用户，包括借还条款、邮件以及现场确认，具体如下：

1. 在用户归还设备时，由服务台工作人员扫描设备二维码。

2. 向用户展示关于数据抹除的确认信息，由工作人员指引用户刷卡确认。

3. 借还系统通过 API 向 Jamf 发送清除的单个设备数据的请求，如果此时设备处于脱机状态则在设备下次联网时执行清除动作。同时，借还系统通过 API 向 Jamf 发送修改设备扩展属性值为 Returned 的请求，该设备将被放到 Returned smart group，遵循该组不能使用任何 App 的策略 。

4. 如果归还的是笔记本，其清除和配置时间较长，需要工作人员保持其电源处于接通状态、网络处于连接状态。

如果未通过借还系统获取设备，那么设备处于 Returned smart group 中，其将无法正常使用。超过借用时长的设备会被系统自动锁定，当用户如需延长时，可以由 IT 远程协助。

通过 Jamf 系统和 ASM 的应用，解决了学校在 Apple 设备管理上的问题，实现了对所有设备的全生命周期管理，规范和简化了管理流程，改善了用户使用体验。未来在远程协助和自助借还方面，上海纽约大学将继续研发，以更完善的服务为师生提供便利。CEN（责编：陈荣）

（作者单位为上海纽约大学信息技术部）