惠普设备即服务分析和主动管理

数据管理常见问题

本文回答了惠普设备即服务分析和主动管理数据收集、传输、存储、保留和数据处理相关的常见问题。

目录

惠普设备即服务分析和主动管理——数据管理常见问题

云技术/数据中心

问：　惠普设备即服务分析和主动管理平台利用了哪些云技术和数据中心？

答：　惠普设备即服务分析和主动管理平台在亚马逊网络服务系统 (AWS) 上托管，该系统是一种可扩展的计算基础结构，也是云托管领域公认的领导者。

惠普设备即服务分析和主动管理平台的数据中心位于美国的俄勒冈 (AWS-OR)和德国的法兰克福 (AWS-DE)。在欧洲、中东和非洲 (EMEA) 区域国家的客户数据可托管在德国数据中心。所有其他国家/地区的客户数据可托管在美国的数据中心。虽然客户可能要求在不同的数据中心有单独的承租者托管不同业务部门的数据，但是单个客户“承租者”的所有数据都托管在一个数据中心里。

如需了解 AWS 的更多信息，请访问 https://aws.amazon.com。

问：　在任务和客户方面，每个数据中心起到什么样的作用？

答：　美国和德国的数据中心可以用来区分不同地区的客户，起到区域数据中心的作用。欧洲的客户可能更倾向于使用德国的区域数据中心，而来自其他国家的客户可能更倾向于使用美国的区域数据中心。这两个数据中心让惠普设备即服务分析和主动管理服务可以在各个区域将个人数据进行本地化处理。

惠普设备即服务分析和主动管理服务在美国分析数据中心开展。出于保护数据的目的，所有个人数据在美国分析数据中心传输和存储之前都会清除识别信息。

问：　设备与各种惠普设备即服务分析和主动管理组件之间的数据流是怎样的？

答：　数据流遵循以下过程：

1. 创建帐户后，惠普设备即服务客户将在基于云的惠普设备即服务分析和主动管理门户上注册，该门户在美国和德国的区域数据中心托管。
2. 分析和主动管理软件随后会推送到客户的设备，个人设备进行注册后交由美国或德国区域数据中心的分析和主动管理软件进行管理。
3. 基于云的惠普设备即服务分析和主动管理门户以及设备上的分析和主动管理软件可以捕获数据，然后将数据发送至美国和德国的区域数据中心。
4. 在数据传输到美国分析数据中心之前，美国和德国数据中心维护的个人数据将会清除识别信息，在利用该数据进行分析。
5. 惠普设备即服务分析和主动管理使用基于云的门户，通过将美国分析数据中心已清除识别信息的分析数据与区域数据中心的个人数据和信息相结合，实现其功能——设备管理及分析服务（如工作组健康状况监控、可执行报告、事件和警报）。

惠普设备即服务分析和主动管理——数据管理常见问题

数据收集

问：　惠普设备即服务分析和主动管理服务要收集哪些数据？这些数据会用于什么？

答：　惠普设备即服务分析和主动管理服务收集的数据“类型”既有直接由客户提供的数据，也有自动从设备上基于云的惠普设备即服务分析和主动管理门户，以及分析和主动管理软件收集到的数据。

惠普设备即服务分析和主动管理需要收集以下数据用于执行合同服务：

数据收集目的	已收集数据	已收集数据描述
客户管理	帐户数据	客户购买或注册惠普设备即服务分析和主动管理的方式，由惠普设备即服务分析和主动管理引起的事件相关的联络历史，以及惠普设备即服务分析和主动管理的任何其他信息，都对交易服务（如帐户管理）的执行有直接影响。
确保惠普设备即服务分析和主动管理软件和服务正常运作	应用程序数据	分析和主动管理软件的版本、安装状态、数据共享选择和更新详情。
帐户设置和授权验证	联系信息	个人和/或业务联系信息，包括名字、姓氏、邮寄地址、电话号码、传真号码、电子邮箱地址以及惠普设备即服务分析和主动管理帐户设置和验证、服务授权，以及通知事件和服务电子邮箱地址等其他类似联系信息。
提供预防性 IT 服务维护和管理，以及以客户为中心的报告/报表	设备数据	设备相关的基本硬件信息：计算机、操作系统、内存容量、区域、语言、时区、型号、首次启动日期、设备使用年限、设备制造日期、浏览器版本、计算机制造商、保修状态、唯一的设备识别号，以及因产品而异的其他技术信息。
		电池、磁盘、基本输入 / 输出系统 (BIOS)、惠普 SureStart、显示和图形，即插即用设备和驱动程序、驱动程序错误和驱动程序崩溃、内存、实时时钟、处理器、系统插槽、环境变量、散热、操作系统、网络接口、操作系统和第三方补丁、防病毒和防火墙状态和应用程序、Windows 设备安全配置文件，以及设备管理配置文件及其状态等硬件组件。
		设备上安装的软件应用程序注：我们不会扫描或收集应用程序可能显示的任何文件或信息的内容。
		性能数据：电池、磁盘、CPU、内存和热利用率。
		软件应用程序的使用频率和使用时间，以及软件使用对硬件性能数据（电池、磁盘、CPU、内存和热量使用）的影响。
		网络利用率数据：设备的网络传输速率。

数据收集目的	已收集数据	已收集数据描述
通过查明丢失设备的位置，为设备提供预防性服务维护和管理	位置数据	地理位置数据可启用定位服务。默认为所有客户关闭此功能，客户可以选择在惠普设备即服务分析和主动管理中启用或禁用定位服务。
用户进行身份验证和授权后访问惠普设备即服务分析和主动管理帐户和服务	安全证书	提供用户账号、密码、密码提示，以及验证所需的类似安全信息，方可授权用户访问惠普设备即服务分析和主动管理帐户和服务。

问：　惠普设备即服务分析和主动管理不会收集什么类型的数据？

答：　惠普设备即服务分析和主动管理不会收集以下类型的数据：

- 人口统计信息（国家或语言习惯除外）
- 金融账户信息、信用卡或借记卡号码、信用记录或支付数据
- 社交媒体或网页浏览信息
- 政府发布的身份识别号，如社会保障号码、社会保险号码或身份证号码
- 健康信息
- 敏感数据，如族裔出身、政治信仰、工会会员身份、健康数据、性取向和基因数据

安全性

问：　惠普设备即服务分析和主动管理采取哪些安全措施保护个人数据？

答：　在捕获、传输和存储数据时，惠普设备即服务分析和主动管理运用各种安全技术和程序，保护您的个人数据，以免未经授权访问、使用或披露。其中包括：

1. 存储在美国和德国地区数据中心的数据：
   - 美国和德国地区数据中心包含个人数据的数据库已进行加密。
   - 在这些地区数据中心的安全证书数据（如惠普设备即服务分析和主动管理帐户密码）使用惠普设备即服务分析和主动管理应用程序等级加密和 SHA256 散列法进行加密。
   - 联系数据（即个人和/或业务联系数据，包括客户和/或用户的名字、姓氏、邮寄地址、电话号码、传真号码、电子邮箱地址以及惠普设备即服务分析和主动管理帐户设置和验证、服务授权，以及通知事件和服务电子邮箱地址等其他类似联系信息）会以明文形式存储在美国和德国的区域数据中心。
   - 位置数据（即由惠普设备即服务分析和主动管理捕获的设备实时地理位置）使用惠普设备即服务分析和主动管理应用程序等级加密和 SHA256 散列法进行加密。
2. 存储在美国分析数据中心的数据：设备、应用和位置数据，在美国分析数据中心中进行传输和保存之前，都进行了反识别处理，不会与任何个人存在联系。

数据传输和存储

问： **惠普设备即服务分析和主动管理在不同的数据中心会传输和存储哪些数据类型？**

答： 以下数据类型会传输和存储在不同的数据中心：

数据类别	美国区域数据中心（适用于非欧洲客户）	德国区域数据中心（适用于欧洲客户）	美国分析数据中心（适用于所有客户）
帐户数据	是	是	否
应用程序数据	是	是	是
联系信息	是	是	否
设备数据	是	是	是
位置数据	是	是	是
安全证书数据	是	是	否

问： **在惠普设备即服务分析和主动管理服务中，客户可以选填哪些数据？**

答： 下表列出了可选择的信息：

数据类别	是否选填	备注
帐户数据	否	
应用程序数据	否	
联系信息	详见备注	客户的名字、姓氏、电子邮箱地址和国家信息是客户必须提供的信息。邮寄地址和电话号码是选填的。
设备数据	否	
位置数据	是	
安全证书数据	否	

问：　惠普设备即服务分析和主动管理数据采集的来源和方法是什么？而数据传输的频率如何？

答：　数据采集的来源和方法以及数据传输频率：

数据类别	来源	方法	传输频率
帐户数据	基于云的惠普设备即服务与分析和主动管理门户	这些数据由客户提供，由惠普设备即服务分析和主动管理支持专家输入，或直接由客户在基于云的惠普设备即服务分析和主动管理门户中输入。	实时根据帐户数据更新。
应用程序数据	基于云的惠普设备即服务分析和主动管理门户和软件	自动更新	每 15 分钟根据应用程序数据更新。
联系信息	基于云的惠普设备即服务与分析和主动管理门户	这些数据由客户提供，由惠普设备即服务分析和主动管理支持专家输入，或直接由客户在基于云的惠普设备即服务分析和主动管理门户中输入。	实时根据联系信息更新。
设备数据	分析和主动管理软件	自动更新	• 用于分析的设备数据每天传输一次。 • 用于设置和监控设备管理配置文件及其状态的设备数据，可实时传输，也可根据设备数据更新每天传输一次。
位置数据	分析和主动管理软件可获取设备的实时定位	自动更新	根据对定位数据的变化，实时或每 12 小时更新一次。
安全证书数据	基于云的惠普设备即服务与分析和主动管理门户	该数据由客户在基于云的惠普设备即服务分析和主动管理门户中输入。	实时根据安全证书数据更新。

问：　惠普设备即服务分析和主动管理获取、传输和存储哪些位置数据？

答：　客户地址数据

- 在惠普设备即服务分析和主动管理中，惠普设备即服务客户可以通过基于云的惠普设备即服务分析和主动管理门户输入他们的地址信息来指示客户的地址。例如：国家、城市、邮政编码、街道地址等。
- 这些信息由客户在基于云的惠普设备即服务门户中手动输入。
- 这些信息不是强制提供的。
- 这些信息只会被传输和存储在美国或德国的区域数据中心。

操作系统国家数据

- 在惠普设备即服务分析和主动管理中注册的设备的操作系统区域。
- 该数据从使用惠普设备即服务分析和主动管理软件的设备上自动获取。
- 这些信息只会被传输和存储在美国或德国的区域数据中心和美国分析数据中心。

实时设备位置数据

- 设备的实时地理位置（如：设备的纬度和经度）
- 只有在惠普设备即服务客户从基于云的惠普设备即服务分析和主动管理门户中启用定位服务时，才会获取该数据。
- 该数据从使用惠普设备即服务分析和主动管理软件的设备上获取。
- 这种基于位置的服务可以在所有客户的惠普设备即服务分析和主动保护默认关闭的情况下，精准找到设备的地理位置；客户可以在基于云的惠普设备即服务分析和主动管理门户中，选择启用或关闭基于位置的服务。即使打开了基于位置服务，惠普设备即服务分析和主动管理也不允许员工任何类别设备或个人设备收集设备位置数据（在基于云的惠普设备即服务分析和主动管理门户中）。
- 这些数据会被传输和存储在美国和德国的区域数据中心。与位置数据相关联的个人数据（即可用于分析的由惠普设备即服务分析和主动管理获取的设备实时地理定位）在传输和存储在美国分析数据中心之前会经过消除识别信息处理。

资产追踪位置数据

- 惠普设备即服务分析和主动管理能够让客户使用基于云的惠普设备即服务分析和主动管理门户输入资产的位置信息。这不是实时的设备位置数据，而是一个标识资产物理位置的标签。例如：1 号楼、 2 楼等。
- 该信息由客户在基于云的惠普设备即服务分析和主动管理门户中手动输入，然后传输和存储在美国或德国区域数据中心和美国分析数据中心。

问：　惠普设备即服务分析和主动管理会如何处理环境变量设备数据中的个人数据？

答：　环境变量可能包含在某些变量值中的个人名称。分析和主动管理从设备中读取已注册的 Windows 用户名，如果该用户名在环境变量值中，则会传输和存储到美国分析数据中心之前将其删除。

但是，如果用户提供的用户名不是在环境变量值中已注册的 Windows 用户名，则在将数据中心环境变量值传输和存储到美国分析数据中心之前，该服务将无法删除该用户名。

例如，如果用户名为 John Boe，而注册的 Windows 用户是 jboe，并且其中一个环境变量值是 C:\Users\jboe\Documents，那么设备上的分析和主动管理软件会将这些数据传输和存储为 C:\Users\username\Documents。但是，如果环境变量值为 C:\Users\john\Documents，那么分析和主动管理会在美国分析数据中心将这些数据传输和存储为 C:\Users\john\Documents。

问：　惠普设备即服务分析和主动管理会如何处理 Windows 事件日志设备数据中的个人数据？

答：　设备的 Windows 事件日志可能包含个人数据。由于数据量大而且种类繁多，所以很难推断、删除和/或清理所有传输和并存储在美国分析数据中心的 Windows 事件日志数据中的个人数据。分析和主动管理不会在其分析或输出中利用来自 Windows 事件日志的任何个人数据。

数据保护

问：　数据是通过公共网络利用 TLS 1.1 或更高版本、IPsec 或其他行业标准强加密技术进行传输加密的吗？

答：　惠普设备即服务分析和主动管理利用 TLS 1.2 在设备与美国和德国区域数据中心以及美国分析数据中心之间传输数据。

问：　数据（数据库、日志、配置文件、备份媒体等）存储是否安全？

答：　美国和德国地区数据中心存储个人数据的所有数据库均已加密。

美国分析数据中心的所有数据库和非结构化存储都将在 2018 年上半年进行加密。

问：　个人数据（数据库、日志、配置文件、备份媒体等）会以明文形式存储

答：　美国和德国地区数据中心存储个人数据的所有数据库均已加密。

此外，在美国和德国的区域数据中心，惠普设备即服务分析和主动管理还为安全证书数据（如帐户密码和实时设备位置数据）提供应用程序级加密和 SHA256 散列法处理。

联系信息（包括用于设备即服务分析和主动管理账户个人和/或业务的客户和/或用户名字、姓氏、邮寄地址、电话号码、传真号码、电子邮箱地址等，）会以明文形式存储在美国和德国的区域数据中心。

问：　数据不再需要时，是否会安全地进行处理？

答：　在美国和德国区域数据中心的所有数据会在客户从惠普设备即服务分析和主动管理服务停用后 30 天内永久删除。

美国分析数据中心的数据会在数据创建之日起五年后删除（注：出于保护数据的目的，在传输到美国分析数据中心进行存储之前，所有个人数据都会清除识别信息。）

问：　如何限制访问数据？

答：　所有收集和存储在美国和德国区域数据中心以及美国分析数据中心的数据都会由亚马逊网络服务系统 (AWS) 通过 IAM 角色、认证用户和桶策略加以保护。

问：　惠普设备即服务分析和主动管理是否会与惠普供应商共享数据？如果是，其中是否包含个人和匿名化的信息？

答：　是的，惠普设备即服务分析和主动管理会与惠普的部分关键供应商共享性能数据（磁盘、CPU、内存），以实现惠普产品的性能优化。惠普仅提供经过汇总的匿名数据，不会涉及任何惠普设备即服务分析和主动管理的客户。

问：　惠普设备即服务分析和主动管理是否会提供单独的专用数据库，让客户使用其专属数据？

答：　不会。

问：　客户数据和信息是否会与其他组织或公司的数据在同一台物理服务器上共同托管？

答：　是的。

4AA7-2191CHP，2018 年 2 月 8 日