实施由身份定义的工作空间的几大技术提示

预计到 2020 年，全球移动办工人员的数量将从 2014 年的 13.2 亿增加到 17.5 亿[1]。如今，越来越来多的移动办工人员依靠多种设备和应用来完成任务，比如，台式机、智能手机、平板电脑，或者办公机械和企业物联网（IoT）设备。并且，员工希望正常登录旧版应用、桌面应用、移动应用、软件即服务（SaaS）应用和云计算应用以及从中注销，具体取决于机会、交互风格或最适合用于完成当前任务的工具集。

最成功的数字化工作空间将会集成信息体系结构，在终端用户访问应用时基于个人身份标识以及每个时间点的情境为其提供简单的体验。身份标识在当今的移动世界中至关重要，这是因为，绑定到单个设备和网络的时代已经一去不复返了。所谓身份标识，不仅是指个人拥有单个域登录名并被授予所有访问权限。移动办公意味着工作不再是仅在企业网络上进行。IT 部门要做的不再是简单地为数据中心设置防火墙。各公司需要围绕用户构建新的安全边界，以消除那些导致无法随时随地进行工作的障碍。如今，几乎每个应用和每项服务都可能要求进行专门的身份验证。

什么是 VMWARE WORKSPACE ONE?

VMware Workspace™ ONE™ 将身份标识和移动化管理相结合，使员工能够随时随地从他们选择的任何设备无阻力地安全访问工作所需的全部应用和数据。要了解有关 Workspace ONE 的更多信息，请访问 https://workspaceone.com。

企业应负责满足这些需求并迎接数字化转型；这对用户和企业都有利。考虑到这一点，下文提供了几大技术提示，用于帮助您将所部署的 VMware Workspace ONE 打造成为最出色的平台，用作身份标识定义的工作空间：

1. 实现跨不同设备无缝访问应用和数据

以 Salesforce 为例，通过交付和配置 Salesforce 原生移动应用，将使用户可以通过 Workspace ONE Web 门户以及公司管理的或“自带”（BYO）移动设备单点登录（SSO）到位于其企业台式机、企业笔记本电脑及个人 PC 上的 Salesforce Web 应用，从而轻松实现跨不同设备无缝访问应用和数据。

2. 确保在员工处于任何状态时 BYO 设备上的数据都始终是安全的

终端用户希望公司向他们选择的任何设备（包括 BYO 移动 iOS 和 Android 设备）交付应用、桌面和移动应用。然而，很显然的是，公司需要确保在用户从公司离职或丢失设备时 BYO 移动设备上的数据仍旧是安全的并且能够从用户设备中擦除数据。

Workspace ONE 能够在终端用户需要其他访问权限时根据需要以自适应方式管理和注册设备。如果终端用户只需要访问企业基本应用，他们可以通过 Workspace ONE 进行登录，并通过 Workspace ONE 单点登录进行身份验证。如果需要提高应用访问的安全程度，Workspace ONE 则会出于企业数据和应用管理目的要求注册设备，从而确保企业数据的安全。如果设备丢失或者用户从公司离职，通过取消注册（根据用户或企业 IT 部门的请求）即可移除数据，且不会影响终端用户移动设备上的其他内容。

1 Strategy Analytics：“Global Mobile Workforce Forecast, 2015-2020”，2015 年 11 月 3 日。

vmware®

3. 使终端用户能够在保持安全性的同时轻松登录

许多终端用户不愿意在他们的移动设备（包括笔记本电脑、平板电脑和智能手机）上进行复杂的配置和多轮身份验证（如 RSA SecurID 和其他 Token 身份验证方法），这是可以理解的。Workspace ONE 使用 VMware Identity Manager™ 安全应用 Token、多因素身份验证功能以及 VMware Verify，因而能够提供易于使用的单点登录功能，如果需要，还支持使用多因素身份验证。

安全的应用 Token 功能针对不同的平台（例如，Cloud KDC for iOS、Android for Work 和 Chrome Tabs for Android，以及 Windows Account Provider 和 TBAUTH）使用不同的技术。

4. 通过与第三方身份标识提供程序集成来整合数字化身份标识的数量

Ping 等第三方身份标识提供程序 (IdPs) 可以与 VMware Identity Manager 一同配置，以便将终端用户身份验证“链接”在一起。例如，Ping 将是 Salesforce 的 IdP，充当服务提供程序。为了通过 VMware Identity Manager 将各种终端用户身份验证链接在一起，Identity Manager 会成为 Ping 的 IdP，Ping 则充当服务提供程序。

示例工作流：

1. 来自 Salesforce 的请求发送至 Ping。
2. Ping 根据用户、应用（桌面应用与移动应用）等因素决定策略。
3. Ping 适配器对桌面用户进行身份验证。
4. Ping 将移动请求转发至 VMware Identity Manager。
5. VMware Identity Manager 决定策略。
6. 设备使用移动身份验证端点进行身份验证。
7. 重新定向回到 Ping。
8. Ping 向 Salesforce 发出 SAML 断言。
9. 成功。

5. 通过连接器轻松集成外部企业系统

VMware AirWatch® Cloud Connector™ 和 VMware Identity Manager Connector 均能对终端用户启用单点登录身份验证。对于每个连接器而言，单点登录身份验证的实现方式都是独一无二的。

VMware AirWatch Cloud Connector (ACC) - 当使用 SaaS Identity Manager 租户时，或者需要单点登录到 SaaS、基于 Web 的应用或移动应用时，应考虑使用 ACC。

这可将用户从本地 Active Directory 同步到 VMware AirWatch 租户。该 VMware AirWatch 租户可将这些用户和组同步到 VMware Identity Manager，从而对用户进行身份验证，以使用户能够访问 Workspace ONE。ACC 仅需要出站 TCP 443 连接。

制胜法宝有两个：消费级简便性与企业级安全性。

VMware Identity Manager Connector - 当部署 VMware Identity Manager 的内部组件时，或者当您需要将 Identity Manager SaaS 租户与 VMware Horizon®、VMware ThinApp® 或 Citrix XenApp 和 XenDesktop 环境集成以单点登录到与基于 SaaS 和/或基于 Web 的应用结合使用的环境时，应考虑使用 VMware Identity Manager Connector。

这可将用户从本地 Active Directory 同步到 VMware Identity Manager 租户。Identity Manager Connector 将支持“仅出站”通信模式，当使用必要的云部署身份验证方法（如密码、RSA 自适应身份验证、RSA SecurID 或远程身份验证拨入用户服务 [RADIUS]）时，仅使用 TCP 443 出站连接与 SaaS Identity Manager 租户进行通信。其他身份验证适配器（如 Kerberos (KerberosIdpAdapter)）仍需要 TCP 443 入站连接，该入站连接将为内部 VMware Identity Manager Connector 使用外部公共网络地址转换成的 IP 地址和公共主机域名全称 (FQDN)。此外，VMware Identity Manager 的内部组件会自动在单一虚拟设备 (SVA) 中部署连接器。

两种 - 如果需要两种移动应用（以及与 VMware Horizon、ThinApp 或 Citrix XenApp 和 XenDesktop 环境进行集成），则既需要 VMware AirWatch Cloud Connector 又需要 VMware Identity Manager Connector。

注意： Workspace ONE 支持 SaaS 和 Web 应用的所有配置。

为什么采用身份标识定义的工作空间?

- 将本地部署和云计算服务的身份标识联合起来。
- 消除用户体验中的冲突。
- 为与情境相适应的规则引擎提供持续安全保护。
- 默认情况下允许访问。
- 为进行授权和身份验证而启用单一信息交流中心。
- 验证设备的合规性状况。

关于 VMWARE IDENTITY MANAGER

VMware Identity Manager 是一款“身份认证即服务”(IDaaS) 产品，可提供应用调配、自助服务目录、条件访问控制等功能，还可提供适用于 SaaS 应用、Web 应用、云计算应用和原生移动应用的单点登录功能。

其优势包括：

- 通过任意设备以一触式访问来简化移动商务
- 利用 VMware AirWatch 优化用户体验并提高安全性
- 通过自助应用商店提升员工的能力
- 值得信赖的 VMware 企业级混合云计算基础架构

有关 VMware Identity Manager 的更多信息，请访问 http://www.vmware.com/cn/products/identity-manager.html。

结束语

利用数字化工作空间，用户可以随时使用任何桌面或设备（自带设备或企业提供的设备），IT 管理员也可以安全地以实时方式自动分发和更新应用。部署身份标识定义的工作空间的企业很容易接受异构性，因为身份标识访问和个性化是超越于每个应用、每台设备之上的。

VMware Workspace ONE 是一个平台集，包含许多解决方案，如 VMware AirWatch®、Socialcast™ by VMware、VMware Horizon Enterprise Edition、ThinApp、VMware User Environment Manager™、VMware App Volumes™ 和 VMware Identity Manager。

事实上，VMware Identity Manager 是整个 Workspace ONE 解决方案的底层支持基础，可将 Workspace ONE 旗下的所有产品和解决方案结合起来。VMware Identity Manager 还为终端用户提供单点登录体验，使他们可以登录到他们所有的远程服务、桌面和应用，其中包括旧版 Windows 应用、托管和远程应用及桌面（包括 Citrix）、基于 SaaS 和基于 Web 的应用，以及移动应用、内容和设备管理。

试用 Workspace ONE，只需几分钟即可在浏览器中启动并运行它，无需进行任何安装。立即查看动手练习。

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com
威睿信息技术（中国）有限公司
中国北京海淀区科学院南路 2 号融科资讯中心 C 座南楼 1 层 邮编：100190 电话：+86-10-5993-4200
中国上海办公室 上海市淮海中路 333 号瑞安大厦 804-809 室 邮编：200021 电话：+86-21-8024-9200
中国广州办公室 广州市天河路 385 号太古汇一座 3502 室 邮编：510610 电话：+86-20-87146110
中国香港公司 香港港岛东太古城太古湾道 12 号太古城中心 4 期 4 楼 电话：852-3696 6100 传真 852-3696 6101 www.vmware.com/cn