管理ACTIVE DIRECTORY的经济和运营成本

Quest®

简介

毫无疑问，Active Directory是您IT基础架构中非常关键的元素之一。企业的日常工作大部分都以正常运行且高效的Active Directory基础架构为中心。从早上支持用户登录或发送电子邮件到提供对文件共享或SharePoint站点等网络资源的访问，Active Directory无处不在。在其正常运行时，人人都感到满意。但是如果其无法正常运行，则很明显：用户无法登录，桌面设置出错，无法访问文件，管理员无法管理用户帐户，等等。

Quest

为了避免这些难题，IT专业人员及管理层投入了大量时间和资源来妥善管理并维护Active Directory。通常，这些任务属于以下主要类别：

- 帐户管理
- 安全管理
- 审核和变更控制
- 组策略
- 备份和恢复
- Active Directory运行状况

所面临的挑战是寻找更具经济效益且运营高效的方式来处理这些任务。正如我们随后将看到的，以上每个方面都存在实际的运营成本。为新用户设置妥当需要花费时间和金钱。精心设置的组策略不仅需要公司投入时间和金钱从备份GPO中恢复或对其重新进行配置，还需要投入时间和金钱为受影响的最终用户恢复工作效率。

此外，雪上加霜的是，这些任务通常由不同的团队进行处理，而这些团队通常使用自己的工具集，这种情况在大型组织中尤为突出。所使用的工具可能是Microsoft管理控制台等原生工具，Windows PowerShell脚本或者旧的批处理或VBScript文件等内部开发的解决方案，也可能是由独立软件供应商提供的专门解决方案。但是，对于整个组织来说，不足之处在于其可能要投入超出满足这些需求所必需的时间和金钱。例如，某个第三方解决方案可能需要额外的后端服务，这意味着会产生其他费用。另一个第三方解决方案可能需要复杂且昂贵的许可方案。如果某个组织利用多个解决方案来应对以上所列的主要方面，则很可能出现一些重叠情况，这意味着为相似的功能重复付费。

我们将了解这些主要方面，并了解如何提高经济效益和运营效率。实际上，是由相同的管理员团队来处理这些任务还是分发工作负载无关紧要；IT专业人员及其各自的管理层需要在关注和支持Active Directory方面保持大局观。

无论什么团队执行Active Directory管理，提高经济效益和运营效率都至关重要。

在本文中，我们将以一家虚构的制造公司为例，该公司具有500个用户和同等数量的计算机，他们分散在两个站点，每个站点具有一些域控制器。当然，这种规模的公司会有一些IT管理员，但是，但我们要分析的是如何通过平均年薪为87,653美元（时薪大约为42.00美元）的单个Active Directory管理员来完成所有管理工作。我们将忽略福利和加班等方面的额外成本。

主要Active Directory管理任务的成本

帐户管理

毫无疑问，Active Directory的核心功能是创建和管理用户、计算机和组。雇用新用户，晋升员工，以及终止一些员工的雇用关系。所有这些活动都需要与Active Directory进行交互。如果我们示例中的IT专业人员使用的是原生工具Active Directory用户和计算机(ADUC)，那么他绝对无法实现高效管理。使用ADUC执行常见任务非常耗时。该工具需要长达10分钟的时间来创建新用户帐户，并将其放置在适当的组中。如果您需要维护审核跟踪（将在后面予以介绍），则所需的时间会更长。

创建单个生产级PowerShell工具大约会花费IT专业人员16个小时的时间。您的公司进行此工作需花费多长时间?

使用Windows PowerShell脚本等内部开发的工具可以缩短一些时间。但是，仍需要花费时间来学习PowerShell、维护脚本以及培训新雇用的IT管理员。当然，这假定IT人员事先具有时间和专业知识来开发这样的解决方案。据我的经验，创建单个生产级质量的PowerShell工具需要8-16个小时。对于我们虚构的IT专业人员来说，这需要投资超过600美元，此外还需要花费时间来获得所需的经验或专业知识。如果该公司必须引进外部专家，则成本很可能会为上述成本的10倍之多。

除了设置新帐户和删除旧帐户之外，管理员还必须投入大量时间进行帐户更改。员工结婚或离婚，需要变更姓名。他们迁至新的办公室，需要更新电话号码。员工晋升，需要更新职位。根据您的组织结构，晋升还可能涉及将用户或计算机物品移至新的组织单位 (OU) 并更改组成员关系。所有这些更改都需要花费时间手动完成，而且易于出现人为错误且代价高昂。

在典型的一个月中，我们的IT专业人员很可能会至少花费30小时来处理这些基本任务。表1展示了这家具有500个用户的公司在典型的一个月中的情况。

每月	活动数量	每个活动的分钟数	总时间（分钟）	总时间（小时）	总成本
新建用户	25	10	250	4.17	175美元
用户变更	125	10	1,250	20.83	875美元
终止	20	5	100	1.67	70美元
组管理	15	10	150	2.50	105美元
总计	185	不适用	1,750	29.17	1,225美元

表*1.* 典型每月帐户管理费用

总之，该公司每月为基本和必要的管理花费1,200美元（每年14,000美元）！公司不能避免这些任务，因此只能设法提高运营效率，从而直接带来经济效益。例如，如果某个新用户帐户可以在1分钟而不是10分钟内完成创建，则在此一项任务上每年便可直接节省1,800美元。当您聚合此整个表中的节省时，就能看到一些实际的好处。

即使是小型公司，如果依赖原生工具的话，也很容易就会在基本用户配置任务方面每年花费14,000美元。

Quest

安全管理

当然，除了处理新用户和组，还有其他Active Directory管理任务。另一个常见运营费用是处理用户密码。在大多数组织中，帮助台接到来电的主要原因是与密码相关的问题。重置密码会花费一些时间。使用ADUC（Active Directory用户和计算机管理控制台）时，至少需要5分钟才能重置用户的密码或解锁其帐户。该时间很容易就会快速增加，具体取决于其他报告或审核要求。在我们的示例公司中，即使我们在计算中仅假定15%的员工需要密码方面的帮助且保守地假定每个活动花费5分钟，这也会每月占用IT 6.25小时的时间。结果是每年花费3,000美元以上。

另一个安全相关的Active Directory任务是委派。在大型组织中，将组织单位的控制委派给其他用户或组的情况并不罕见。委派可针对整个OU或OU中特定类型的对象，例如打印机。某些委派可能非常精细，例如委派可为OU中的帐户重置用户密码的人员。在ADUC中完成这些委派非常耗时，而且不一定直观。当然，这不一定是频繁出现的Active Directory管理任务，但是每次很容易就花费10分钟的时间才能完成。

而更加困难的方面是了解现有的委派以及对其进行更改。ADUC不是合适的选择，其无法全面地显示已委派的内容和委派对象。一些IT专业人员依靠内部开发的PowerShell脚本或命令行工具。其他公司则投资于另一个管理工具，该工具通常按用户进行许可。如果我们的IT管理员每月在委派或权限相关的任务上花费1个小时，则该公司每年的直接费用为500美元。

如果您一直在统计的话，会发现公司在基本Active Directory管理方面花费的费用为每年17,500美元。一方面，可能有人认为这是IT管理员的薪酬。从某种程度上说是这样，但我认为这种想法比较短视。如果IT管理员受制于效率不佳的工具和做法，则不仅会产生直接经济成本，还会产生因管理员忙于确定谁有权限更改用户密码而未完成的某些事项所导致的损失成本。诚然，IT专业人员无论怎样都将获得薪酬，但是如果他们有机会处理可使公司受益或提升管理员专业水平的其他任务或项目，那么人人都会受益。

但是，我们只是做了初步工作。甚至仅在满足管理需求方面，原生工具都无法提高效率。

审核和变更控制

对于许多组织来说，审核以及某种形式的变更控制即使不是完全的强制要求，也是非常重要的事项。您是否了解谁在Active Directory中创建了用户帐户？谁在何时修改了组的成员关系？坦率地讲，在Active Directory审核和变更控制方面，没有Microsoft原生工具。许多管理员求助于第三方工具来梳理事件日志以收集此类型的信息，或者依靠PowerShell脚本来实现相同的目标。无论采用何种方式，公司都必须投资于为第三方审核工具进行许可或投入管理员时间。如果超负荷的IT专业人员必须追查过去一个月已创建、修改和删除的帐户数，则可能需要花费8-10小时的时间。

而收集到该信息后，几乎总是需要将其格式化为某种类型的报告。同样，没有原生工具可执行此操作，因此我们只能使用内部开发的脚本，这或许是创建Microsoft Excel电子表格或寄希望于第三方管理工具包含报告功能。

除了变更控制外，IT管理层通常希望获得有关Active Directory当前状态的报告。在我作为IT顾问的职业生涯中，我发现组织会创建有关以下各个方面的报告：

- 即将过期的密码
- 具有不会过期密码的用户
- 为空和未使用的组
- 某个用户所属的组
- 属于域管理员组的用户
- 过时的计算机帐户
- 过时的用户帐户
- 按部门列出的用户
- 按OU列出的用户
- 按成本中心列出的用户
- OU权限

没有Microsoft原生工具来帮助您进行Active Directory审核和变更控制。

几乎对于所有这些报告，ADUC的价值都非常有限，因此IT专业人员通常求助于脚本和第三方工具。这通常意味着直接许可成本以及了解如何使用新工具处理每项任务所花费的时间。在我们虚构的公司中，IT管理员每月很容易就花费5小时进行审核、变更控制和报告，这导致每年产生2,500美元以上的费用。很明显，可以缩短时间而不牺牲质量的任何事情都值得考虑。

Quest

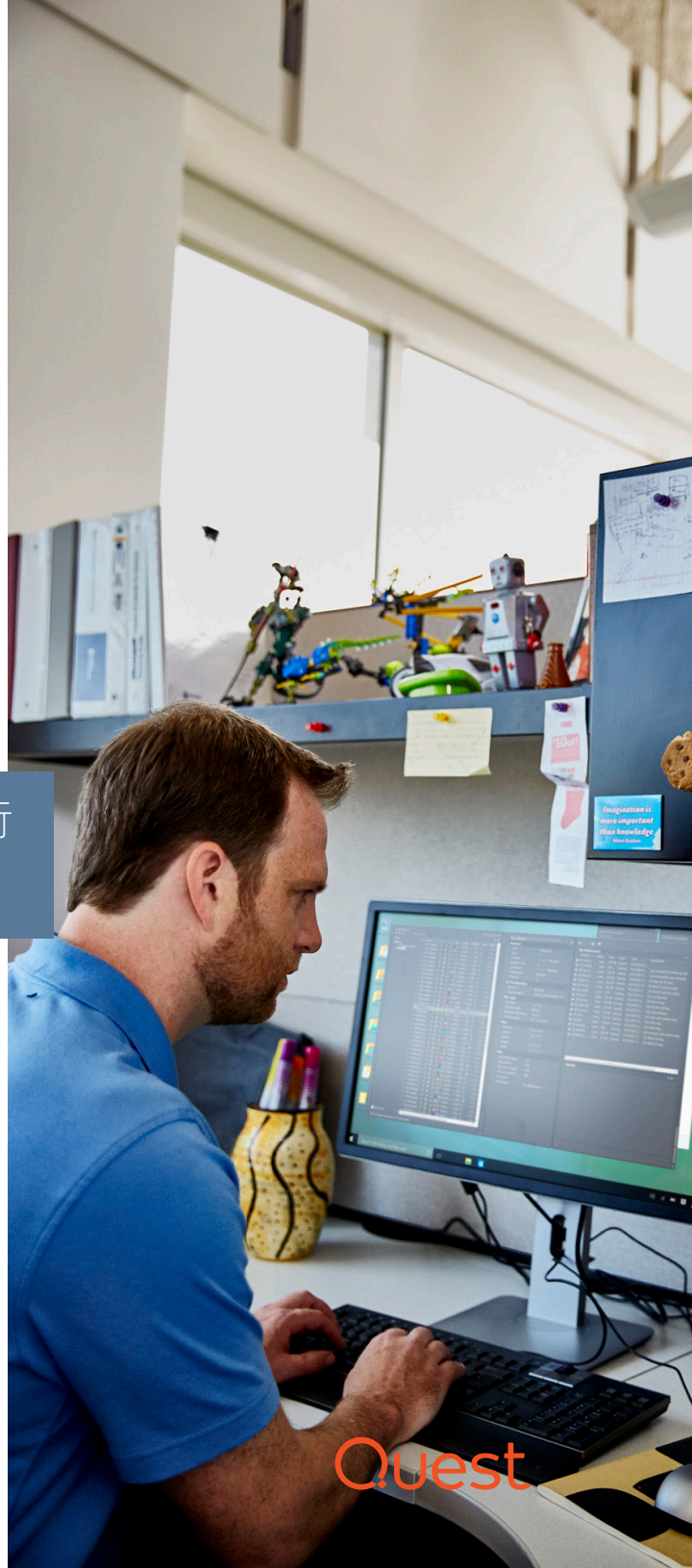
组策略管理

另一个Active Directory相关的任务是关注和支持组策略。不幸的是，这又是一个严重缺乏原生工具的方面。组策略管理控制台可以很好地执行基本任务，但是无法很好地进行扩展。通过管理控制台管理单个GPO非常耗时，无论您需要进行备份还是创建报告都是如此。Microsoft提供一组PowerShell cmdlet，可用于管理组策略，但是它们不直观，需要一些PowerShell经验，而且功能有限。例如，如果您要比较两个GPO，则是一项非常复杂的任务，需要 一些非常丰富的PowerShell经验。

正确实施的组策略是公司的资产，并可节省资金。但是很遗憾，即使其推出已超过18年，仍有许多组织不使用它，而且我相信这与缺乏实用的原生管理工具及其所需的时间直接相关。唯一的替代方式是寻找符合您的需求的第三方组策略工具，而且您可能会找到多个工具。

> 组策略管理控制台可以很好地执行基本任务，但是无法很好地进行扩展。

我们的IT管理员需要定期备份GPO，并且偶尔需要进行恢复。我们估计他平均每月花费2小时来执行该任务，每年相应的费用为1,000美元。此外，他在对帮助台问题进行故障排除时，需要不时地使用组策略，通常会比较GPO版本来发现潜在问题。其中一些工作可以通过原生管理控制台来完成，但是可能每月需要大约90分钟来执行GPO相关的工作。突然，管理Active Directory中的组策略每年就需要公司花费超过1,700美元，更不用说由于组策略问题可能导致的员工工作中断，这也会产生直接成本。



备份和恢复

由于Active Directory具有任务关键性，因此需要定期备份。备份不仅是实现业务连续性所必需的，也是为了提供保护以免受到事故和人为错误的影响。意外删除OU及其所有用户帐户是很容易发生的事情。不幸的是，通过原生工具备份Active Directory却并不轻松。如果ADUC提供“自我备份”这样的功能就再好不过了，可惜并没有。有命令行工具可以使用，但是它们非常复杂。即使使用脚本解决方案，Active Directory备份也非常耗时。

如果备份非常繁琐，那么从备份进行恢复就会更加糟糕。不久以前，您可能仍存在这样的情况（具体取决于您的Active Directory版本）：从Active Directory恢复删除的项目是非常耗时的过程。您必须在AD恢复模式下重新启动域控制器。追查恢复模式密码。追查备份文件。恢复备份。使用复杂的命令行工具配置恢复。重新启动并期待最好的结果。即使您需要恢复单个删除的用户帐户，此过程可能轻易就花费一两个小时的时间。

最后，Microsoft提供了Active Directory回收站功能，稍微缩短了该过程，但不一定更加轻松。使用此功能需要Windows PowerShell，因为没有图形界面。您还需要确切了解需要恢复的内容。同样，替代方式是投资于Active Directory备份解决方案。不足之处在于这会产生其他许可成本，以及需要IT员工学习新的工具。

这对我们困惑的IT管理员意味着什么？我估计在备份Active Directory、定期测试恢复以及偶尔需要恢复某些内容方面，他每月大约花费4小时，公司因此每年产生大约2,000美元的成本。这无疑是通过适当工具便可大大提高效率并最终降低成本的一个方面。

Quest

ACTIVE DIRECTORY运行状况管理

最后，典型的Active Directory管理任务是非常重要的一项任务：监控总体运行状况。域控制器是否在正常运行？复制是否按预期工作？名称解析是否正常运行？所有操作主角色是否均在线？这些只是IT管理员必须处理的日常任务中的一部分。不幸的是，在原生工具方面，他必须使用多种工具，而没有一种工具具有合适的报告功能。有一些命令行工具，但是这些工具需要一些专业知识才能正确使用，而且为大多数这些任务编写PowerShell脚本只有经验非常丰富的脚本编写员和管理员才能够胜任。

为了监控AD的运行状况，IT管理员必须使用多个原生工具，而没有一个工具具有合适的报告功能。

对于其他管理方面，有第三方工具可以处理其中一些任务。但是，请注意许可成本。即使产品按域控制器或管理员进行许可，但如果有合理的用户与域控制器和管理员比率，则我更喜欢将成本转换为每个用户的成本。在我们的示例制造公司中，IT管理员每月很容易就会花费8小时的时间来监控Active Directory，此外还需要在对问题进行故障排除时花几个小时。总体来说，这会使公司每年产生4,000美元的成本，因为他必须依靠原生工具以及从互联网上获取且不甚了解的一些PowerShell脚本。

为什么原生工具和点式解决方案不是具有成本效益的方法?

现在，我们精疲力尽的虚构管理员每月花费50-60小时来艰难地管理Active Directory，并让每个人感到满意。他使用手动工具进行的工作很容易出错，而且非常耗时。但是我的计算结果是，具有500个用户帐户的公司每年需要的成本在25,500美元以上。这是效率不佳仅影响该管理员的情况，但是通常还有其他某个人（例如高管或用户）正在等待，因此实际成本要高得多。 此外，50-60小时的IT时间不能用于别处。

另外，我仅计算了虚构的公司在少数几个方面如何管理Active Directory。理想情况下，组织需要管理Active Directory的所有方面。他们需要了解他们当前流程的效率如何以及有效成本。哪些本应完成的任务由于缺乏人力资源或预算而未完成？许多公司尝试进行的快速解决方法是在内部开发临时解决方案。在当今许多Microsoft商店中，这意味着求助于Windows PowerShell。现在，不要误解；PowerShell是出色的管理工具，可以填补许多管理缺口。但是，在构建完整PowerShell解决方案方面涉及的工作非常艰巨，需要丰富的经验，而且很可能仅适合大型组织。总之，如果您尝试仅使用Windows原生工具来管理Active Directory，则会花费大量精力、时间和资源。这些工具不是为当今的企业专门设计的。

认识到原生工具无法提高效率后，公司可能决定在一些主要方面投资于专用解决方案。但是，此方法存在一些潜在的风险。首先是许可的经济现实。为了使计算简单，我们假设他们购买的工具的平均成本为每个用户8.00美元。那么对于500个用户，这意味着每年12,000美元的成本。只有此工具可将管理员的工作量每月减少23小时，此成本才算合理。

> 部署多个点式解决方案成本高昂，因为每个解决方案都会产生许可费用、安装和维护费用以及培训成本。

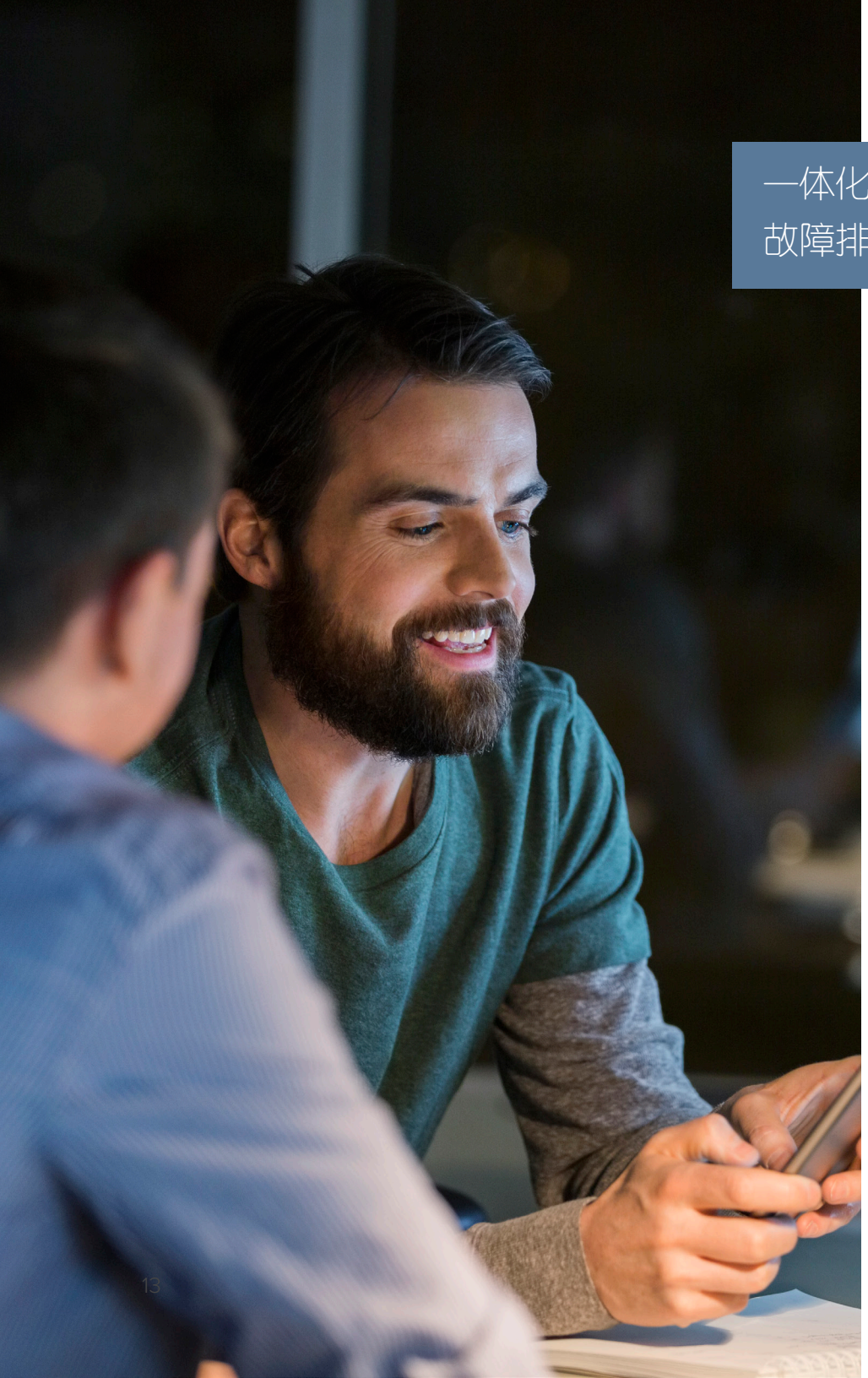
第二，安装三个不同的工具会产生其他关联的成本。一些工具可能需要安装代理。一些工具可能需要其他后端费用，如新的Web服务器。一些工具可能需要安装在域控制器上，而其他工具则在管理员的桌面中。关键在于，多个工具将需要部署和维护多个资源。

最后，三个不同的工具具有学习曲线，而且每次雇用新管理员时都必须重复该学习曲线。即使这些成本难以量化，但是不可忽略。

使用一体化的Active Directory管理解决方案

这会为我们超负荷的IT专业人员及其公司带来怎样的局面？投资于一体化Active Directory管理工具是更好的方法。此解决方案应至少适用于上面讨论的方面：帐户管理、安全、变更控制、组策略、备份和恢复以及运行状况监控。我发现并不是每个公司都会管理所有这些方面。例如，您的公司可能较小，以至还没有如火如荼地开始使用组策略。不过您仍需要提前进行规划以备将来使用。目标是为IT人员提供单个要学习的工具，尤其是您使用或计划使用基于角色的访问控制(RBAC)时。好处是，每个人都学习可保持必要的管理隔离的通用工具，但是当需要角色交叉或新的访问时，学习曲线非常短。这有助于从一开始便提高IT管理员的效率。自然，如果单个管理解决方案无法提高效率并最终降低运营成本，就不值得投资；它应将任务时间缩短至数分钟。

一体化的管理解决方案还具有更高的成本效益，因为我们将进行单次安装和配置 - 通常应用程序是集成的，因此所有不同的方面都可共享通用基础架构。这应当有助于降低总体成本。我们虚构的公司仅是为三个点式解决方案支出的直接许可成本就超过12,000美元，而单个全面的管理解决方案可能只需9,000美元。当然，此解决方案必须即时大幅提高效率。在当今的敏捷环境中，企业不再奢望具有长期投资回报。



一体化AD管理解决方案不仅可简化AD管理，还可加速故障排除，提高安全性与合规性，以及促进决策。

一体化Active Directory管理解决方案可以使日常管理它的IT专业人员实现突破。帮助台团队通常利用Active Directory和组策略进行故障排除；随时可访问Active Directory相关的信息可缩短修复时间，从而降低管理成本并提高最终用户的效率。安全与合规性团队还通常需要利用Active Directory来完成其被分配的任务。拥有全面的解决方案对于这些人员来说非常宝贵，因为这些方面的Windows原生工具非常糟糕。以额外成本对另一个产品进行许可没有业务意义。最后，实用的一体化解决方案可服务于IT管理。用于任何类型报告的原生工具都严重缺乏，或需要许多临时开发工作。但是没有足够多切实可行的信息，管理层无法做出明智的业务决策。这是另一个可能难以量化的隐形成本，但它真得不容忽视。

Quest

结论

总之，Active Directory管理是持续不断的一系列任务关键型任务。尝试通过Windows原生工具来完成这些任务非常耗时、易于出错且无法很好地进行扩展。这甚至是在假定原生工具能够处理任务的前提下！我已通过明显虚构的数字（但这些数字都源于现实经验）展示了产生运营费用的方面。您应使用我的示例作为指导准则来分析您自己的效率和费用。您现在执行什么管理任务以及它们花费多长时间？哪些任务由于您缺乏时间或资源而未执行？使用当前管理工具集的运营成本是多少？不管您使用的是原生工具还是第三方解决方案，都会产生后端费用，例如培训、许可和额外硬件费用。请使用您自己的财务数据，您很可能会对实际费用感到惊讶。

请花时间计算您在AD管理方面的成本；
您很可能对实际成本感到惊讶。

最后，还有无形的总体满意度标准。员工和管理层是否对他们使用的工具感到满意？他们要处理的任务是否超出了当前工具集的功能范围？他们花费了多少时间和精力来克服效率不佳的问题？您的IT专业人员是乐于关注Active Directory还是对其有些害怕？

有许多方法可用来进行Active Directory管理。请确保您在经济效益和运营方面都非常高效的方式妥当地进行该管理。

关于作者

Jeffery Hicks是拥有近30年经验的IT资深专家，其大部分职业生涯都作为IT基础架构顾问，专攻Microsoft服务器技术，且重点研究自动化和效率。他多年荣获Microsoft MVP大奖。现在，他的职业为独立作家、教师兼顾问。Jeff向全球各地的IT专业人员教授和展示了PowerShell以及自动化的优势。他独立撰写和联合撰写了多部图书；为许多在线站点供稿；而且是Petri.com的特约编辑、Pluralsight作家，经常在技术研讨会和用户组会议中发表演讲。您可以在Twitter上关注Jeff (http://twitter.com/JeffHicks)，以及关注他的博客(https://jdhitsolutions.com/blog)。

关于QUEST

Quest致力于为瞬息万变的企业IT领域提供软件解决方案。我们帮助简化数据爆炸、云扩展、混合数据中心、安全威胁以及合规要求所带来的挑战。我们是一家全球性服务提供商，向遍及100个国家/地区的130,000家企业提供服务，其中包括95 %的财富500强企业以及90 %的全球1000强企业。自1987年以来，我们构建了丰富的解决方案产品组合，现在包括数据库管理、数据保护、身份和访问管理、Microsoft平台管理以及统一端点管理。借助Quest，企业可以缩短IT管理时间，将更多时间用于业务创新。有关详细信息，请访问：www.quest.com。

如果您对可能使用的本材料存有任何问题，请联系：
www.quest.com/cn-zh/company/contact-us.aspx

Ebook-ManagingEconomicCostsAD-US-GM-zh_CN-WL-37551

Quest