

5个步骤增强活动目录的安全 PDF转换可能丢失图片或格式，
建议阅读原文

https://www.100test.com/kao_ti2020/243/2021_2022_5_E4_B8_AA_E6_AD_A5_E9_AA_A4_c100_243829.htm 活动目录（AD）中保存着能够对AD进行访问的重要密钥，如果不能恰当地增强AD的安全性，那么它很容易受到攻击。坦率地讲，增强AD的安全性并不简单，但是通过一些基本的步骤，您确实可以提高它的安全性。请注意我这里所说的是"基本"步骤。安全无止境，您总是可以找到提高安全性的方法，但是这些方法往往需要付出相应的代价。这些代价可表现为实际的花费，或者灵活性或功能性方面的损失。让我在这里向您展示5个步骤，实施这些步骤的代价并不算高，但它们却可以帮助您切实增强AD基础设施的安全性。

步骤1. 遵循管理员方面的最佳做法您可以通过将手工操作（例如，安装域控制器）自动化的方法来增强AD的安全性，但是目前还没有出现能够将人类行为自动化的程序设计语言。因此，这就是您需要为管理员如何管理AD建立指南的原因。您需要确信您的管理员遵循了如下的最佳做法：区分管理账号（administrative accounts）的使用。区分管理账号的使用已经成为许多组织的一个标准做法，但它仍然值得一提。如果管理员的机器不小心感染了病毒，那么潜在的威胁将会非常大，因为获得管理权限（right）后，病毒可运行程序或脚本。因此，对于日常操作，管理员应使用非特权账号（例如，用户账号）；对于和AD有关的操作，管理员应使用一个独立的管理账号。当您通过一个非管理账号登录后，您可以使用Runas命令这类工具以管理员的身份打开程序。如需了解有关如何使用Runas命令的信

息，请参阅Windows的帮助文件。确保管理员机器的安全性。虽然要求您的管理员以非管理账号登录和使用Runas命令打开AD管理程序能够带来很多益处，但是如果运行这些工具的硬件系统不安全的话，您仍然处于危险之中。如果您不能确保管理员机器的安全性，那么您需要建立一个独立并且安全的管理员机器，并让管理员使用终端服务来访问它。为了确保该机器的安全，您可以将它放在一个特定的组织单元中，并在组织单元上使用严格的组策略设置。您还需要注意机器的物理安全性。如果管理员的机器被盗，那么机器上的所有东西都将受到威胁。定期检查管理组（administrative group）的成员。攻击者获得更高特权（privilege）的手段之一就是将其账号添加到AD的管理组当中，例如Domain Admins、Administrators或Enterprise Admins。因此，您需要密切关注AD管理组中的成员。遗憾的是AD不具备当某个组的成员发生改变时发送提示信息的内建机制，但是编写一个遍历组成员的脚本并使脚本每天至少运行一次并不复杂。在这些组上面启用审核（Enabling Auditing）也是一个很好的主意，因为每次改变都会在事件日志中有一条对应的记录。限制可以访问管理员账号（Administrator account）密码的人员。如果某个攻击者获得了管理员账号的密码，他将获得森林中的巨大特权，并且很难对他的操作进行跟踪。因此，您通常不应使用管理员账号来执行管理AD的任务。相反，您应该创建可替代的管理账号（alternative administrative accounts），将这些账号添加到Domain Admins或Enterprise Admins组中，然后再使用这些账号来分别执行每个管理功能。管理员账号仅应作为最后一个可选择的手段。因为它的使用应该受到严格的限

制，同时知道管理员密码的用户数量也应受到限制。另外，由于任何管理员均可修改管理员账号的密码，您或许还需要对该账号的所有登录请求进行监视。准备一个快速修改管理员账号密码的方法。即使当您限制了可以访问管理员账号的人数，您仍然需要准备一个快速修改该账号密码的方法。每月对密码进行一次修改是一个很好的方法，但是如果某个知道密码（或具有修改密码权限）的管理员离开了组织，您需要迅速对密码进行修改。该指南同样适用于当您在升级域控制器时设置的目录服务恢复模式（Directory Service Restore Mode，以下简称DSRM）密码和任何具有管理权力的服务账号。DSRM密码是以恢复模式启动时用来进行登录的密码。您可以使用Windows Server 2003中的Ntdsutil命令行工具来修改这个密码。当修改密码时，您应该使用尽量长的（超过20个字符）随机密码。对于管理员而言这种密码很难记忆。设置完密码后，您可将它交给某个管理人员，并由他来决定谁可以使用该密码。准备一个快速禁用管理员账号的方法。对于绝大多数使用AD的组织，最大的安全威胁来自于管理员，尤其是那些对雇主怀恨在心的前管理员。即使您和那些自愿或不自愿离开公司的管理员是好朋友，您仍然需要迅速禁用账号上的管理访问权限。

步骤2. 遵循域控制器方面的最佳做法

在确信遵循了与管理员有关的最佳做法后，我们将注意力转移到域控制器（Domain Controller，以下简称DC）上面来，因为它们是所有AD实现中最容易受到攻击的目标。如果某个攻击者成功进入DC，那么整个森林将受到威胁。因此，您需要遵循如下最佳做法：确保DC的物理安全性。DC的物理安全性是部署AD时需要考虑的最重要问题之一。如果某个攻击

者获得了DC的物理访问权，他将有可能对几乎所有其它的安全措施进行破坏。当您把DC放置在数据中心时，DC的安全性并不存在问题；当在分支机构部署DC时，DC的物理安全性很可能存在问题。在分支机构中，DC经常存放在可以被非IT人员访问的带锁房间内。在一些情况下，这种方式不可避免，但是不管情况如何，只有被充分信任的人员才能够对DC进行访问。

自动化安装的过程。通常自动化任务的执行要比手工执行的安全性高。当安装或升级DC时尤其如此。安装和配置操作系统过程的自动化程度越高，DC的不确定因素就越少。当手工安装服务器时，对每台服务器人们的操作均存在细微的差别。即使完整地记录下所有过程，每台服务器的配置仍然会有所区别。通过安装和配置过程的自动化，您有理由确信所有DC均以同样的方式被配置并设置安全性。对于已经安装好的DC，您可以使用组策略这类工具来确保它们之间配置的一致性。

迅速安装重要的更新。在Windows NT时代，除非绝对需要，绝大多数管理员不会安装热修复程序（hotfix）或安全更新。更新经常存在缺陷并会导致进一步的问题。今天，我们就没有那么奢侈了。幸运的是微软提供的更新程序质量有了很大提高。因为DC是非常显眼的目标，所以您需要密切关注出现的每一个安全更新。您可以通过自动更新（Automatic Updates）迅速地对安全更新进行安装，或者通过微软的Software Update Services（SUS）在测试后有选择地对其进行安装。

创建一个保留文件。在Windows Server 2003以前的操作系统中，如果用户具备在某个容器中创建对象的权限，那么将无法限制用户创建对象的数量。缺乏限制可以导致攻击者不断地创建对象以至耗尽DC硬盘空间。您可以通过

过在每个DC的硬盘上创建一个10M至20M的保留文件，以便在某种程度上降低这类风险的发生。如果DC的空间用完了，您可以删除上述保留文件，并在找到解决方案前留下一些解决问题的空间。运行病毒扫描软件。在DC上运行病毒扫描软件比在大多数服务器上运行该软件更为迫切，因为DC间不仅要复制目录信息，还要通过文件复制服务（File Replication Service，以下简称FRS）复制文件内容。不幸的是FRS为病毒提供了在一组服务器之间进行传播的简单途径。并且FRS通常还会对登录脚本进行复制，因此还会潜在地威胁到客户端的安全。运行病毒扫描软件可以大幅降低病毒复制到服务器和客户端的威胁。100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com