实施“基于角色的访问控制”（RBAC）：五步走

非官方中文译文·安天技术公益翻译组 译注

简译版

文档信息			
原文名称	5 steps to simple role-based access control (RBAC)		
原文作者	Robert C. Covington	原文发布日期	2019 年 1 月 2 日
作者简介	Robert C. Covington 是togoCIO.com 的创始人兼总裁。 https://www.csoonline.com/author/Robert-C.-Covington/		
原文发布单位	CSO Online		
原文出处	https://www.csoonline.com/article/3060780/access-control/5-steps-to-simple-role-based-access-control.html		
译者	安天技术公益翻译组	校对者	安天技术公益翻译组
分享地址	请浏览创意安天论坛 bbs.antiy.cn 安天公益翻译板块		
免责声明	• 本译文译者为安天实验室工程师，本文系出自个人兴趣在业余时间所译，本文原文来自互联网的公共方式，译者力图忠于所获得之电子版本进行翻译，但受翻译水平和技术水平所限，不能完全保证译文完全与原文含义一致，同时对所获得原文是否存在臆造、或者是否与其原始版本一致未进行可靠性验证和评价。 • 本译文对应原文所有观点亦不受本译文中任何打字、排版、印刷或翻译错误的影响。译者与安天实验室不对译文及原文中包含或引用的信息的真实性、准确性、可靠性、或完整性提供任何明示或暗示的保证。译者与安天实验室亦对原文和译文的任何内容不承担任何责任。翻译本文的行为不代表译者和安天实验室对原文立场持有任何立场和态度。 • 译者与安天实验室均与原作者与原始发布者没有联系，亦未获得相关的版权授权，鉴于译者及安天实验室出于学习参考之目的翻译本文，而无出版、发售译文等任何商业利益意图，因此亦不对任何可能因此导致的版权问题承担责任。 • 本文为安天内部参考文献，主要用于安天实验室内部进行外语和技术学习使用，亦向中国大陆境内的网络安全领域的研究人士进行有限分享。望尊重译者的劳动和意愿，不得以任何方式修改本译文。译者和安天实验室并未授权任何人士和第三方二次分享本译文，因此第三方对本译文的全部或者部分所做的分享、传播、报道、张贴行为，及所带来的后果与译者和安天实验室无关。本译文亦不得用于任何商业目的，基于上述问题产生的法律责任，译者与安天实验室一律不予承担。		

实施“基于角色的访问控制”（RBAC）：五步走

Robert C. Covington

2019 年 1 月 2 日

“基于角色的访问控制”（Role-based Access Control，RBAC）是指根据员工在机构中的“角色”为其分配系统访问权限。需要注意的是，并非每位员工都需要担任主角。

且不论我们遭遇的各种高级网络攻击场景，即使在一些简单的问题上，我们也似乎一直在“搬起石头砸自己的脚”。

举例来说，《2017 年威瑞森数据泄露调查报告》发现，在与黑客攻击相关的数据泄露事件中，81%涉及凭证泄露。此外，正如 Crowdstrike 公司《2018 年入侵服务案例手册》所述，简单的故障可能会导致系统性的影响。在该报告中，他们列举了这样一个案例：一家大型跨国服装公司的一名员工，在一家咖啡店里使用公共网络处理工作。结果，该员工的凭证遭泄露，导致整个公司的基础架构受到损害。

为什么看似简单的访问控制实施起来会这样困难呢？也许，它只是看似简单而已。我们以一家只有 20 名员工和 5 个系统的公司为例。假设对于每个系统，员工的访问权限分为：“读取文件”、“读取/写入文件”、“管理权限”或“无权限”。那么，在如此小的环境中，就有大量的访问设置排列组合。

更糟糕的是，在典型的小型公司中，访问权限的管理过于随意，甚至“一刀切”。如此看来，访问权限的管理也不是那么简单的。但是，如果我们无法有效地管理访问权限，就很难保护系统的安全。

解决这一问题的方法可以追溯到 20 世纪 70 年代，早在大多数人了解信息安全之前就出现了。该方法称为“基于角色的访问控制”（RBAC）。根据美国国家标准与技术研究院（NIST）发布的文献，第一个正式的 RBAC 模型是在 1992 年提出的。因此，多年来我们一直拥有强大的解决方案。

RBAC 是什么？

RBAC 是指根据员工在机构中的“角色”为其分配系统访问权限。首先，分析员工的系统访问需求，并根据相同的工作职责和系统访问需求将其分为若干角色。然后，严格根据角

色为员工分配访问权限。这样一来，访问管理就会容易很多。

即使有这样一种可实现的、历史悠久的方法，我们似乎还是无法驾驭访问控制，这是为什么呢？当然，我们正朝着 RBAC 的方向努力。重要的行业标准，包括《支付卡行业数据安全标准》（PCI DSS）、《医疗电子交换法案》（HIPAA）和《格雷姆-里奇-比利雷法案》（Gramm-Leach-Bliley），都要求某种形式的 RBAC。

我认为，RBAC 不常被使用的一个原因是：对于中小型公司来说，当员工加入公司时，临时分配访问权限似乎更容易。问题在于，即使公司只有少量系统，也会存在大量的访问设置组合排列，因此这种方法不具备可持续性。

RBAC 有什么优点？

适当地实施 RBAC，可以使访问权限的分配变得系统化和可重复。此外，审计用户权限和纠正所发现的问题也会容易得多。

RBAC 可能听起来令人生畏，但实际上它很容易实现，并且会使访问权限的持续管理变得更加容易和安全。

毕竟，企业努力预防的数据泄露可能正是源自内部。

RBAC、ABAC 和 ACL

RBAC 有一些替代方案，包括：

访问控制列表（ACL）。ACL 是指为给定用户或用户组授予特定对象（如文档）的访问权限。举一个简单的例子，ACL 允许一个部门的用户对文档进行更改，同时只允许其他部门的用户读取该文档。

基于属性的访问控制（ABAC）。ABAC 也称为“基于策略的访问控制”，是指通过各种属性，包括用户所在部门、时间、访问位置、所需访问类型等，来确定是否应该向用户授予访问权限。

除了 RBAC 的基本概念，上述两种方案还提供额外的控制粒度，但是它们也极大地增加了创建和维护必要权限所需的工作量。RBAC 可以提供更加简化和可管理的方法，可以将某个用户的权限，授予处于同一角色的其他所有人。此外，这些方法可以协同使用以增强控制。

实施 RBAC：五步走

希望通过上文，你已经对 RBAC 产生了兴趣。接下来，可以通过以下五步来实施 RBAC。

1. 盘点企业系统

如果你还未盘点需要控制访问权限的资源，请尽快着手盘点。这些资源包括电子邮件系统、客户数据库、联系人管理系统、文件服务器上的主要文件夹等。

2. 分析员工并创建角色

企业可以根据相同的访问需求，将员工分为不同的“角色”。需要注意，不要定义过多的角色，尽可能保持简单化和层次化。

企业可能拥有基本的用户角色，这类角色涵盖所有员工都需要的访问权限，例如电子邮件和内网的访问权限。另一类角色是“客户服务代表”，此类角色需要对客户数据库的读取/写入权限。“客户数据库管理员”则可以完全控制客户数据库。

3. 向员工分配角色

创建角色并确定其访问权限后，企业需要确定每个员工所属的角色，并为其设置相应的访问权限。

4. 避免“一次性”更改访问权限

企业应避免对具有异常访问需求的员工进行一次性的权限更改。此惯例一开，企业的 RBAC 系统将会很快瓦解。企业应根据需要更改角色，或在必要时添加新角色。

5. 审计

定期检查各个角色及其所涵盖的员工，以及访问权限。例如，如果你发现某个角色具有对特定系统的非必要访问权限，请更改角色，并调整该角色中所有员工的访问权限级别。

例如，在医疗记录的访问方面，医疗机构需要遵守相应的法规，因此许多医疗机构使用 RBAC 来准确定义各类医护人员的访问权限。医生可以无限制地访问其患者的医疗记录，但是接待员只需访问患者的基本联系信息。鉴于大量工作人员处于层次化的角色中，因此 RBAC 可以有效控制医疗记录的访问，同时遵守 HIPAA 法案和其他法规。

有些工具可以帮助企业设置 RBAC。许多系统（例如微软活动目录）具有内置角色，企业可以以其为起点，并根据自己的实际情况进行扩展。企业还可以使用身份管理系统，根据

角色自动分配权限。

安天简介

安天是引领威胁检测与防御能力发展的网络安全国家队，始终坚持自主先进能力导向，依托下一代威胁检测引擎等先进技术和工程能力积累，研发了智甲、镇关、探海、捕风、追影、拓痕等系列产品，为客户构建端点防护、边界防护、流量监测、导流捕获、深度分析、应急处置的安全基石。安天致力于为客户建设实战化的态势感知体系，依托全面持续监测能力，建立系统与人员协同作业机制，指挥网内各种防御机制联合响应威胁，实现从基础结构安全、纵深防御、态势感知与积极防御到威胁情报有机结合，推动客户整体安全能力建设的叠加演进。安天为网信主管部门、军队、保密、部委行业和关键信息基础设施等高安全需求客户，提供整体安全解决方案，产品与服务为载人航天、探月工程、空间站对接、大飞机首飞、主力舰护航、南极科考等提供了安全保障。

安天是全球基础安全供应链的核心赋能方，全球近百家著名安全厂商、IT 厂商选择安天作为检测能力合作伙伴 ,安天的威胁检测引擎为全球超过三十万台网络设备和网络安全设备、超过十四亿部智能终端设备提供了安全检测能力。

安天技术实力得到行业管理机构、客户和伙伴的认可，已连续五届蝉联国家级安全应急服务支撑单位。安天是中国应急响应体系中重要的企业节点，在“红色代码”、“口令蠕虫”、“心脏出血”、“破壳”、“魔窟”等重大安全威胁和病毒疫情方面，实现了先发预警和全面应急响应。安天针对“方程式”、“白象”、“海莲花”、“绿斑”等几十个高级网空威胁行为体及其攻击行动，进行持续监测和深度解析，协助客户在“敌情想定”下形成有效防护，为捍卫国家主权、安全和发展利益提供了有力支撑。

2016 年 4 月 19 日，在习近平总书记主持召开的网络安全和信息化工作座谈会上，安天创始人、首席架构师作为网络安全领域的发言代表，向总书记进行了汇报。2016 年 5 月 25 日，习近平总书记在黑龙江调研期间，视察了安天总部，并对安天人说，“你们也是国家队，虽然你们是民营企业”。

安天实验室更多信息请访问： *http://www.antiy.com（中文）*

http://www.antiy.net（英文）

安天企业安全公司更多信息请访问： *http://www.antiy.cn*

安天移动安全公司（AVL TEAM）更多信息请访问： *http://www.avlsec.com*