第5章

访问控制技术

本章学习目标

- 了解访问控制的基本概念
- 掌握自主访问控制和强制访问控制的相关知识
- 掌握零信任架构、基于角色的访问控制和基于属性的访问控制的相关知识
- 掌握配置 Ranger 安全组件实现访问控制

随着计算机技术的发展和网络的广泛应用，信息的获取和处理越来越便捷，信息的共享程度越来越高，极大地推动了社会发展，同时也为不法分子非法使用系统资源开启了方便之门。访问控制技术是计算机科学与安全工程的结合体，也是保证网络安全的核心技术之一。

本章首先向读者介绍访问控制的基本概念以及相关术语。然后，针对主流的自主访问控制、强制访问控制，详细介绍其概念、特点、相应的策略以及经典模型，并对零信任的概念、结构及对应的基于属性与基于角色的两种访问控制模型进行具体介绍。最后，在 Linux 环境下，对配置 Ranger 安全组件实现大数据访问控制的操作过程进行详细介绍。

5.1 概　　述

访问控制是实现既定安全策略的系统安全技术，它管理所有资源的访问请求，即根据安全策略的要求，对每一个资源访问请求做出是否许可的判断，能有效防止非法用户访问系统资源和合法用户非法使用资源。

在信息化时代，网络化程度不断提高，云计算、物联网等新兴技术不断应用于生活之中，大数据的价值不言而喻。在大数据不断为我们创造经济价值的同时，也需要同时注重大数据面临的安全问题。访问控制技术是保证数据安全的重要技术，通过访问者的权限限制对访问者的操作进行监控，防止访问者的操作破坏系统的安全性。访问控制的主要目的是对访问者的身份进行识别，确定访问者的资格和权限，如果访问者是合法用户，会被授权访问目标系统中的资源，同时访问控制系统会保证访问者不会对目标系统的安全造成影响。对于访问者的越权请求，访问控制系统会拒绝访问者。用户的所有访问行为都是在审计监督下进行的，访问者的每个操作都会被记录，访问者的操作行为记录可以为相应的安全问题解决提供数据支持。访问控制是针对越权使用资源的防御措施，是重要

的网络安全防范策略，主要任务是控制用户可否进入系统以及进入系统的用户能够读写的数据集。

访问控制的发展经历了自主访问控制、强制访问控制、基于角色的访问控制、基于属性的访问控制等阶段。其中，自主访问控制是产生最早，也是最基本的一种访问控制技术，至今仍有大量应用；政府、军队等安全性要求较严格的机构则多采用强制访问控制；在商业领域，基于角色的访问控制目前应用最为广泛；基于属性的访问控制则适用于多安全域的互联网应用。自主访问控制、强制访问控制、基于角色的访问控制都需要预先获取用户的身份信息，然后再根据其身份或者该身份所绑定的安全标记、角色等信息进行访问控制判定。后来，提出了基于属性的访问控制，它无须预先知道访问者的身份，而是通过安全属性来定义授权，具有较高的动态性和分散性，能够较好地适应开放式环境。

访问控制策略是主体对客体的访问规则集，它直接定义了主体对客体可以实施的具体行为和客体对主体的访问行为所做的条件约束。访问控制策略的任务是保证网络资源不被非法使用和非法访问。访问控制模型是对访问控制策略及其作用方式的一种形式化表示方法，也是一种从访问控制的角度出发，描述系统安全，建立安全模型的方法。访问控制模型定义了主体、客体和访问是如何表示和操作的，它决定了授权策略的表达能力和灵活性。授权策略是访问控制的关键，用于确定一个主体是否能访问客体的一套规则。本章 5.2 节、5.3 节分别介绍自主访问控制与强制访问控制的相关定义、特点、访问控制策略以及访问控制模型。

随着云计算、大数据、物联网等新兴技术的不断兴起，企业 IT 架构正在从“有边界”向“无边界”转变，传统的安全边界逐渐瓦解。与此同时，零信任安全逐渐进入人们的视野，成为解决新时代网络安全问题的新理念、新架构。5.4 节将对零信任安全理念的内容、网络架构、逻辑组件进行介绍。5.5 节和 5.6 节对两种基于零信任概念引申并发展的访问控制模型——基于角色的访问控制与基于属性的访问控制，从概念、架构等方面进行介绍。

然而，在大数据应用场景下，大数据的规模和增长速度以及应用的开放性，使得安全管理员对访问控制的权限管理越来越困难。同时，数据应用需求的不可预测性也使得管理员无法预先制定恰当的访问控制策略。因此，访问控制技术迫切需要自动化的授权管理和自适应的访问控制，以使其满足大数据场景的需求。为了应对这些问题，提出了基于数据分析的访问控制技术，本章 5.7 节从中选取角色挖掘技术、风险自适应的访问控制技术进行了详细介绍。

在大数据应用中，系统的规模和复杂性使得管理员自上而下地进行角色定义变得越来越困难，而角色挖掘这种自底向上的自动化角色定义方式就为大数据应用中实施基于角色的访问控制提供了有效途径。不仅基于角色的访问控制中的角色可以从数据中挖掘，其他访问控制技术的权限相关要素(甚至权限本身)也可以从数据中挖掘。

风险自适应的访问控制技术的目的在于解决预先定义的静态访问规则和未来不可预期的访问控制需求之间的矛盾，为访问控制提供权限控制的灵活性。本章将介绍风险要素选取、量化计算方法等风险量化的细节内容。传统访问控制的“允许/拒绝”二值判定并不能很好地体现权限控制的灵活性。因此，本章介绍采用风险带的访问控制判定方法，风

险与收益的平衡机制等。最后,针对一些需要实施静态且严格的访问控制规则的应用场景,又介绍了风险访问控制和其他访问控制技术结合的方法。

5.1.1 访问控制的术语

在访问控制研究的历史进程中,逐渐发展出一些用于描述访问控制模型和系统的术语。

1. 用户

用户(User)是指使用计算机系统的人,从另外一个层面上也指计算机中的账号等。在许多系统设计中,一个用户可以拥有和同时使用多个登录账号。授权机制保证了这些账号都能获得与用户相匹配的权限。只有安全管理认可的有效用户才能够登录到系统中,而不同级别和类型的用户拥有不同的访问权限,从而保证信息系统的安全性。

一般情况下,用户大致可以分为以下4类。

① 特殊的用户:系统管理员,其具有最高级别的特权,可以访问所有资源,并且具有所有类型的访问操作能力。

② 普通的用户:其访问操作受到一定限制,而且他的权限由系统管理员分配。

③ 作审计的用户:负责整个安全系统范围内的安全控制与资源使用情况的审计。

④ 作废的用户:曾经有权使用系统,但现在遭到系统拒绝的用户。

其中,作为特殊用户的系统管理员在计算机系统中具有极为重要的战略意义,与信息系统的安全密切相关。系统管理员用户具有对计算机系统进行全面更改、在系统中安装程序和访问计算机上的所有文件等功能。拥有系统管理员用户是取得该计算机上其他用户账户的完全访问权的前提。具体来说,系统管理员具有以下权限。

(1) 可以创建和删除计算机上的用户账户。

(2) 可以为计算机上的其他用户账户创建账户密码。

(3) 可以更改其他用户的账户名、密码和账户类型。

计算机系统中至少有一个用户是系统管理员账户,当一个系统内只有唯一一个管理员账户时,则该管理员账号将没办法把自己的账户类型更改为受限制账户类型。要实现前面的操作,计算机系统中至少还有一个其他用户在该计算机上拥有管理员账户类型。

2. 主体

在计算机系统中,主体(Subject)也被称为访问的发起者。主体是一个可以对资源发起访问的主动实体,人、进程或设备等实体都能成为主体,而通常主体一般指代用户执行操作的进程。实际上,用户对计算机的所有行为都是通过运行在计算机上的进程来实现。即使在一个登录或一个会话这样的简单操作中,一个用户也会产生多个主体。主体的主要作用在于它能引起信息在客体之间流动。例如,在对一个文件进行编辑时,编辑进程是存取文件的主体,对文件这一客体进行编辑的相关操作。再如,一个邮件系统可能在后台运行,定时从服务器收取邮件,当用户登录浏览器查看邮件时,用户的每一步行为都是一个主体,进程的每一次访问都会被检查,以确保这些行为是被用户所允许的。一个主体为

完成任务，可以创建新的主体，这些新主体可以在不同的计算机上运行，并由创建者主体控制它们。

3. 客体

客体(Object)指需要保护的可访问的资源，又称作目标。其中包括可供访问的各种软硬件资源，同时也指接受其他实体访问的被动实体。在信息社会中，客体可以是信息、记录、文件等的集合体，也可以是网络上的硬件设施，在有些文献中也被称为目标，包括文件外设(如打印机)、数据库、细粒度的实体(如数据库表中的某个字段)等。客体是系统中被动的、主体行为的承担者，对一个客体的访问隐含着对其所含信息的访问。系统中最典型的客体是文件或资源，客体的实体类型有程序、程序块、记录、段、文件、页面、目录树和目录，还有视频显示器、处理器、字、字段、位、时钟、键盘、字节、打印机和网络节点等。虽然在早期的访问控制模型中，计算机程序、打印机或其他的活动实体也可能被当作客体，但更多情况下，客体被视为存储或接收信息的被动实体，系统中需要保护的系统资源都可认为是客体，如磁盘等存储介质、远程终端、信息管理系统的事务处理及其应用、数据库中的数据、应用资源等。

在信息系统中，主体和客体的关系是相对的，并不是绝对的，它们在不同情况下可能相互转化。在实际的操作过程中，并不能把系统中的每个实体明确地分为主体和客体。术语“主体”和“客体”只是为了区分一个访问请求中的主动方和被动方而衍生出的概念而已。根据不同的情况，实体可能是某个访问请求的主体，而又是另一个访问请求的客体。主体和客体给出了关注控制的两个选项，可以规定任意一种，即一个主体被允许做什么，或可以对一个客体做什么。

4. 操作

操作(Operation)指主体调用一个程序的过程，从主客体的层面上则是指主体对客体请求的具体行为，包括读、写等动作或行为。在早期的访问控制模型中，所有运行的程序都被认为是主体，但是在后来的基于角色的访问控制模型中，开始区分主体与操作。

5. 权限

权限(Permission)指为了保证职责的有效履行，任职者必须具备的对某事项进行决策的范围和程度，对计算机系统而言则指对计算机某些资源执行某些操作的许可。一旦设置了权限，用户在系统中进行任何一项操作，对资源进行的任一访问都会受到系统的限制，而特定用户对特定资源进行特定操作的许可则是权限的具体体现。比如授予某个主体对计算机资源有读的许可，则代表了一个权限的存在，这个权限表示：获取了对计算机资源的读许可。一般而言，权限包含对客体的许可和对操作的许可两方面内容。对两个客体的相同操作许可，或对同一个客体的两个不同操作许可，均被认为是两个不同的权限。

6. 最小权限

最小权限(Least Privilege)，也称最小特权，是指用户所拥有的权力不能超过他执行

工作时所需的权限。在计算机中，主体在执行操作时，按照主体所需权利的最小化原则分配主体权利。从信息系统的安全层面来讲，应该限定每个主体具有完成任务所必需的最小权限集合，最小权限原则的优点是最大限度地限制主体实施授权行为，这样既可以避免来自未授权主体、错误和突发事件的危险，又可以将可能的错误、网络部件、事故的篡改等原因造成的损失减小到最小。最小权限原则，一方面，给予主体“必不可少”的权限，使所有的主体都能在所赋予的权限之下完成所需要完成的任务或操作；另一方面，它只给予主体“必不可少”的权限，这就在一定程度上限制了每个主体所能够实行的操作。实现最小权限原则，需要分清用户的工作职责，确定完成该工作的最小权限集，然后把用户限制在这个权限集合的范围之内。严格遵守最小权限，需要在不同时间根据任务或功能的执行需求，赋予用户不同程度的许可。虽然在一些情况下，这些限制可能让用户觉得不方便，或者给系统管理员增加许多额外的负担，然而，从信息的保密性和完整性等方面考虑，无论在何种情况下，都不能给予用户或主体超越其职能的权限。

7. 引用监控机

引用监控机(Reference Monitor，RM)是 Anderson 在 1972 年引入的抽象概念，是指系统中监控主体和客体之间授权访问关系的部件。早期的访问控制技术都是基于可信引用监控机的，能够对系统中的主体和客体之间的授权访问关系进行监控。在数据存储系统中存在一个所有用户都信任的引用监控机时，就可以用它来执行各种访问控制策略，实现客体资源的受控共享。

引用监控机是负责实施系统安全策略的硬件与软件的结合体，模型如图 5.1 所示。引用监控机查询授权数据库，以决定主体是否有权对客体进行何种操作，同时将相应活动记录在审计数据库中。

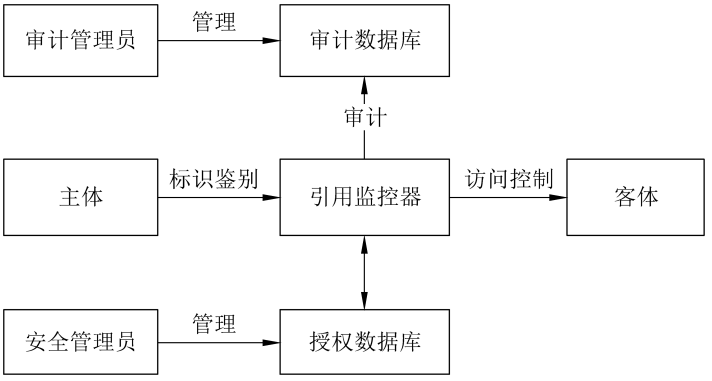

图 5.1 引用监控机模型

8. 引用认证机制

引用认证机制(Reference Validation Mechanism，RVM)是指引用监控机的软硬件实现。引用认证机制是真实系统中访问控制能够被可信实施的基础。

引用认证机制需要同时满足以下 3 个原则。

(1) 必须具有自我保护能力,能够抵抗攻击。

(2) 必须总是处于活跃状态,所有访问行为都受到监控,RVM 不能被绕过。

(3) 必须设计得足够小,以利于分析和测试,从而能够证明它的实现是正确的。

5.1.2 访问控制的目标

访问控制可以实现信息安全的保密性、完整性等目标。

保密性目标:如果主体对客体的所有访问均在访问控制的限制下进行,就可通过对需要进行保密性保护的信息制定相关的访问控制策略,仅允许为了工作需要的主体有权读取相关的客体信息,而未授权者则禁止读取这些客体信息,这样即可达到保密性保护的安全目标。

完整性目标:制定相关的访问控制策略,使得只有授权主体能对确定的客体信息进行修改、插入、删除等写操作,而限制其他主体对这些客体的相应操作权限,即可防止未授权者对客体的篡改、插入、删除等,确保信息的完整性。

访问控制技术必须与其他信息安全技术联动,才能从整体上发挥其应有的安全保护作用。例如,访问控制技术与身份认证技术联动,只有在识别用户真实身份的前提下,访问控制才有意义,用户身份认证的方法可以参看第 4 章的身份认证技术。

5.1.3 访问控制的过程

授权(Authorization)是规定可对该资源执行的动作,包括读、写、执行或拒绝访问,明确是否允许某个用户访问某个系统资源、特定区域或信息的过程,也可以说是资源所有人对他们使用资源的许可。授权是访问控制的重要过程,正确的授权依赖于认证,通过认证来确定你是谁,通过授权来确定你能做什么。

授权过程是确定用户访问权限的机制,通过引用监控机决定访问是否被允许或拒绝。授权是组织运作的核心,它通常以人为对象,将完成某项工作所必需的权力授给部属人员。同时,主管将处理交涉、用钱、用人、做事、协调等决策权移转给部属,不只授予权力,且还托付完成该项工作的必要责任。组织中的不同层级有不同的职权,权限则会在不同的层级间流动,因而产生授权的问题。授权是管理人的重要任务之一,有效的授权是一项重要的管理技巧。若授权得当,所有参与者均可受惠。例如,人力资源的员工通常都被授权允许访问员工档案,在计算机系统中这条策略就会被形式化为一条授权规则。当一个人力资源部员工通过身份认证机制登录到员工档案系统试图修改某人的档案信息时,系统的访问控制机制将检查该用户是否有使用员工档案系统的权限,是否有修改档案信息的权限,并将相关权限赋予该用户。实现授权的方式有很多,访问控制列表(Access Control List,ACL)是其中一种,它将用户与系统资源的访问关系存放在一张表中,可能是给每种系统资源附上一张可访问用户清单,也可能是给每个用户附上一个可访问资源列表。

5.1.4 访问控制的等级划分标准

《信息安全技术 数据安全能力成熟度模型》(GB/T 37988—2019)标准中,基于组织

的数据安全需求和合规性要求，建立身份鉴别和访问控制机制，防止对数据的未授权访问风险，具体安全等级划分如下。

1. 等级 1: 非正式执行

该等级的数据安全能力描述如下。

组织建设：未在任何业务中建立成熟稳定的身份鉴别与访问控制机制，仅根据临时需求或基于个人经验在个别系统中采用了身份鉴别与访问控制手段。

2. 等级 2: 计划跟踪

该等级的数据安全能力要求描述如下。

(1) 组织建设：应由业务团队相关人员负责管理核心业务系统的用户身份及数据权限管理。

(2) 制度流程：核心业务应明确重要系统和数据库的身份鉴别、访问控制和权限管理的安全要求。

(3) 技术工具如下所述。

① 核心业务系统应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，鉴别信息具有复杂度要求并定期更换。

② 核心业务系统应提供访问控制功能，对登录的用户分配账户和权限。

③ 核心业务系统应提供并启用登录失败处理功能，多次登录失败后应采取必要的保护措施。

3. 等级 3: 充分定义

该等级的数据安全能力要求描述如下。

(1) 组织建设：组织应设立统一的岗位和人员，负责制定组织内用户身份鉴别、访问控制和权限管理的策略，提供相关技术能力或进行统一管理。

(2) 制度流程如下所述。

① 应明确组织的身份鉴别、访问控制与权限管理要求，明确对身份标识与鉴别、访问控制及权限的分配、变更、撤销等权限管理的要求。

② 应按最少够用、职权分离等原则，授予不同账户为完成各自承担任务所需的最小权限，并在它们之间形成相互制约的关系。

③ 应明确数据权限授权审批流程，对数据权限申请和变更进行审核。

④ 应定期审核数据访问权限，及时删除或停用多余的、过期的账户和角色，避免共享账户和角色权限冲突的存在。

⑤ 应对外包人员和实习生的数据访问权限进行严格控制。

(3) 技术工具如下所述。

① 应建立组织统一的身份鉴别管理系统，支持组织主要应用接入，实现对人员访问数据资源的统一身份鉴别。

② 应建立组织统一的权限管理系统，支持组织主要应用接入，对人员访问数据资源

进行访问控制和权限管理。

③ 应采用技术手段实现身份鉴别和权限管理的联动控制。

④ 应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现。

⑤ 访问控制的粒度应达到主体为用户级，客体为系统、文件、数据库表级或字段。

(4) 人员能力：负责该项工作的人员应熟悉相关的数据访问控制的技术知识，并能够根据组织数据安全管理制度对数据权限进行审批管理。

4. 等级 4: 量化控制

该等级的数据安全能力要求描述如下。

(1) 制度流程：组织应建立数据安全角色清单，明确数据安全角色的安全要求、分配策略、授权机制和权限范围。

(2) 技术工具如下所述。

① 应建立面向数据应用的访问控制机制，包括访问控制时效的管理和认证，以及数据应用接入的合法性和安全性取证机制。

② 应建立人力资源管理与身份鉴别管理、权限管理的联动控制，及时删除离岗、转岗人员的权限。

③ 应采用技术手段对系统或应用访问敏感数据进行访问控制。

5. 等级 5: 持续优化

该等级的数据安全能力要求描述如下。

技术工具如下所述。

① 应建立针对数据生存周期各阶段的数据安全主动防御机制或措施，如基于用户行为或设备行为的安全控制机制。

② 应参与国际、国家或行业相关标准制定。在业界分享最佳实践，成为行业标杆。

5.1.5 大数据访问控制面临的挑战

1. 安全管理员的授权管理难度更大

在访问控制系统中，一般安全管理员会定义哪些用户对哪些资源具有访问权限。然而，在大数据应用场景中，安全管理员的授权管理难度会急剧增加。其一，由于大数据的规模极大且增长速度极快，安全管理员进行权限管理的工作量也随之快速增多。其二，安全管理员必须具备更多的领域知识来满足在开放式的大数据应用场景下实施权限管理。例如，在医疗大数据场景中，数据集可能包含医生个人信息、患者个人信息、电子病例、社保信息等，而用户则可能包括医院的医生、护士、后勤人员以及各种社保工作人员，甚至包括一些医学研究机构的人员等。相比于之前单独的医疗系统、社保系统或科研支撑系统，安全管理员需要了解更多的领域知识来完成安全标记定义、角色定义或属性定义等权限管理操作。因此，在大数据应用场景中，安全管理员往往难以准确地进行授权，过度授权

和授权不足的现象比较突出。针对这个问题，在大数据应用场景下，安全管理员由于人力和领域知识两方面的限制，迫切需要一些自动化或半自动化的技术来简化其授权管理工作。

2. 严格的访问控制策略难以适用

大数据的一个显著特点是先有数据，后有应用，人们在采集和存储数据时，往往无法预先知道所有的数据应用场景，因此，经常会出现一些新的数据访问需求。若预先定义的访问控制策略过于严格，那么新的访问需求很可能由于不能完全符合允许访问的条件而被拒绝，从而影响大数据系统的可用性。若预先定义的访问控制策略过于宽松，那么虽然系统的可用性得到了保障，但是系统的安全性却大幅降低。因此，在无法预知所有数据访问需求的情况下，严格执行预先定义的访问控制策略是难以实现的，因此，需要一种能够在访问控制过程中自适应地调整权限的技术来解决该问题。

3. 外包存储环境下无法使用

大数据的一种重要存储方式是外包存储，即数据所有者与数据存储服务提供者是不同的，这就产生了数据存储需求与安全需求之间的矛盾：一方面，数据所有者有利用数据存储服务进行数据存储和分享的需求；另一方面，由于不具备在数据存储服务中建立自己信任的引用监控机的能力，也就无法采用上述的早期访问控制技术来确保数据安全。因此，除了采用法律、信誉等手段让数据所有者信任数据存储服务提供者能按照访问控制策略对数据进行保护外，还需要一些技术手段来确保无可信引用监控机场景下的数据安全。密码技术为解决该问题提供了另一条途径，它能够将数据的安全性建立在密钥的安全性基础上，是大数据安全存储研究中的重要方向。

5.2 自主访问控制

5.2.1 自主访问控制的定义及特点

自主访问控制(Discretionary Access Control，DAC)，又称为任意访问控制。作为客体的拥有者的个人用户可以设置访问控制属性来允许或拒绝对客体的访问，那么这样的访问控制就称为自主访问控制。自主访问控制最早出现在20世纪70年代初期的分时系统中，它是在多用户环境下系统最常用的一种访问控制技术。自主访问控制源于这样的理论：客体的主人(即资源所有者)全权管理有关该客体的访问授权，有权泄露、修改该客体的有关信息。自主，即指具有被授予某种访问权力的用户能够自己决定是否将访问控制权限的一部分授予其他用户或从其他用户那里收回他所授予的访问权限。在实现上，首先要对用户的身份进行鉴别，之后根据访问控制列表所赋予用户的权限允许和限制用户使用客体的资源。主体控制权限的修改通常由特权用户或特权用户(管理员)组实现。

自主访问控制允许授权者访问系统控制策略许可的资源，同时阻止非授权者访问资源，某些时候授权者还可以自主把自己拥有的某些权限授予其他授权者，该模型的不足就

是人员发生较大变化时，需要大量的授权工作，因此系统容易造成信息泄露。

自主访问控制面临的最大问题是具有某种访问权的主体能够自行决定将其访问权直接或间接地转交给其他主体。自主访问控制允许系统的用户对属于自己的客体按照自己的意愿允许或者禁止其他用户访问。基于自主访问控制的系统中，客体的拥有者负责设置访问权限，主体的拥有者对访问的控制有一定的权利。由于用户可以任意传递权限，因此没访问文件权限的用户能够从拥有访问权限的用户那里得到访问权限或直接得到文件。因此，自主访问控制模型的安全访问相对较低，不能给系统提供充分的数据保护。

5.2.2 自主访问控制策略

如果普通用户能够参与一个安全性策略的策略逻辑定义与安全属性分配，则称此安全性策略为自主安全性策略。自主访问控制策略根据来访主体的身份，以及“谁能访问、谁不能访问、能在哪些资源上执行哪些操作”等事先声明的访问规则，来实施访问控制。

自主访问控制策略作为最早被提出的访问控制策略之一，至今已有多种改进的访问控制策略。下面介绍传统 DAC 策略和几种由 DAC 发展而来的访问控制策略。

1. 传统 DAC 策略

传统 DAC 策略的基本过程已在上文中介绍过，可以看出，访问权限的管理依赖于所有对客体具有访问权限的主体。很明显，传统 DAC 策略主要存在以下 3 点不足。

(1) 资源管理比较分散。

(2) 用户间的关系不能在系统中体现出来，不易管理。

(3) 不能对系统中的信息流进行保护，容易泄露。

其中，第三点不足对信息系统来说带来的安全威胁是最大的。

针对传统 DAC 策略的不足，许多研究者提出了一系列的改进措施。

2. HRU、TAM、ATAM 策略

早在 20 世纪 70 年代末，Harrison、Ruzzo 和 Ullman 就对 DAC 进行了扩充，提出客体主人自主管理该客体的访问和安全管理员限制访问权限随意扩散相结合的半自主式的 HRU 访问控制模型。1992 年，Sandhu 等为了表示主体需要拥有的访问权限，将 HRU 模型发展为 TAM(Typed Access Matrix)模型。随后，为了描述访问权限需要动态变化的系统安全策略，TAM 发展为 ATAM(Augmented TAM)模型。

HRU 与传统 DAC 最大的不同在于，它将访问权限的授予改为半自主式：主体仍然有权利将其具有的访问权限授予给其他客体，这种授予行为也要受到一个调整访问权限分配的安全策略的限制，通常这个安全策略由安全管理员制定在 HRU 中，每次对访问矩阵进行改变时(包括对主体、客体以及权限的改变)，先生成一个临时的结果，然后用调整访问权限分配的安全策略来对这个临时结果进行判断。如果这个结果符合此安全策略，才允许此次访问权限的授予。HRU 模型基本不会存在非授权者会“意外”获得某个不应获得的访问权限的问题。但这种设定当主体集和客体集发生改变时，需要依赖安全管理员对访问权限的扩散策略进行更新。