思科:三要诀设计基于角色策略访问控制方案Cisco认证考试
 在基于角色访问控制策略的访问控制解决方案中，每个要素都具有重要的作用。因此，在对多因素验证及单点登录解决方案进行验证的时间，每一个要素都需要进行评估。在公司实施解决方案的时间，不要急于对登录方式进行精简而忽略一项或者多项重要测试。 在对网络、系统、网络控制设备进行评估的时间，合并所有类型的身份验证方式，将身份验证和授权统一到基于角色的独立访问控制(RBAC)模式下带来的诱惑会是非常大的。在这个过程中，削减成本(包括执行和管理等方面)通常是重要的推动力。但是，基于角色策略访问控制解决方案的三个要素是服务于不同的特定目的的。因此，在选择访问控制解决方案的时间，设计人员应该从每个要素的角度以及它们之间的关系等多个方面进行全面考虑，以便最终可以实现最佳效果。 在本文中，我将对访问控制解决方案进行简单的介绍，对它们在整体访问控制过程中是如何相互协作进行说明的，并提醒实施者注意在选择访问控制解决方案时，哪些测试是经常容易被忽略的。 定 义 在就如何有效设计基于角色策略的访问控制解决方案进行讨论前，我必须先确定将讨论的问题是正确的，不存在误解或者歧义。 主体和客体。在访问控制解决方案中，主体指的是试图获取资源的实体。这里的资源被称为对象(例如，网络、应用、服务等)。客体的例子包括用户、业务应用软件及操作系统的服务。 身份(识别) 。当一个主体尝试访问一个客体的时间，应该进行的第一个步骤

就是身份识别操作，这实际上就是我们通常说的认证和授权机制。身份识别使用的一些众所周知的方式。 身份验证。一旦主体的身份被确认，它就可以获得已知的东西，或者是获得访问客体的权限。验证的时间，必须确保使用的是没有其他人知道的信息。 授权。获得连接客体的权限必须包含了如何对权限进行管理的问题，这牵扯到主体是怎么使用客体等方面的问题。这种提供角色细化权限的连接方式就是授权。在Windows环境下基于角色策略的访问控制解决方案是怎么工作的 基于角色策略的访问控制解决方案需要制定明确有效的策略。对于数据中心和商业用户来说，在实施基于角色的访问控制解决方案的整个过程中对角色作用进行定义往往是最难最耗费时间的部分。在一个基于微软Windows操作系统的环境下，需要按照业务流程分析和最低权限原则等信息进行处理，以便建立有效的基于角色的访问控制模式，保障系统信息的安全。 首先，我们需要一种方法，将新员工和现有员工的信息统一纳入公司的身份识别系统中。举例来说，生物识别技术、数字证书技术等都是不错的选择。 我们还需要确定对于网络访问或者其它信息资源来说，哪些连接是必要的。 建立一个用户帐户的模板，并将它放到新建或者现有的组、组织单位等位置。这个地方将提供验证访问方式。 创建具有系统级别权限的帐户，用来保存传递身份验证信息的安全应用。确定信息安全策略，对信息进行分级，确保只有拥有相应权限的用户才能查阅相关的信息。 一旦身份识别、身份验证和授权的控制模式开始工作，就可以按照设定的规则对用户进行管理。图一显示的就是一个用户登陆到系统中的整个过程。 用户必须通过的第一道防线是身份识别。通常情

况下，这会是一种基于生物识别技术的解决方案。一旦用户的身份被识别，就来到了身份验证操作的负责范围。一般验证方式采用的是密码、个人识别码等方式，此外，也可以利用位于活动目录中的用户帐户进行验证。 通过了第二道防线后，用户就可以连接网络，浏览普通或者大众类资源了。通过对目录服务进行控制和配置网络设备就可以实现对信息的管理，这包括了下面几个方面： 组成员管理 组织单位处理 组策略对象 虚拟局域网/网段存取控制清单(网络身份验证操作通常是在该装置的基础上进行的) 数字证书 本地目录 举例来说，就象公司的工资系统，不论该应用是否和整体策略存在联系，它也需要利用身份验证模式来确保安全。在特定规则下，用户信息可以安全有效的进行传递。该应用是否采用了单点登陆或者是否使用了活动目录下的数字证书并不是需要关注的问题。 