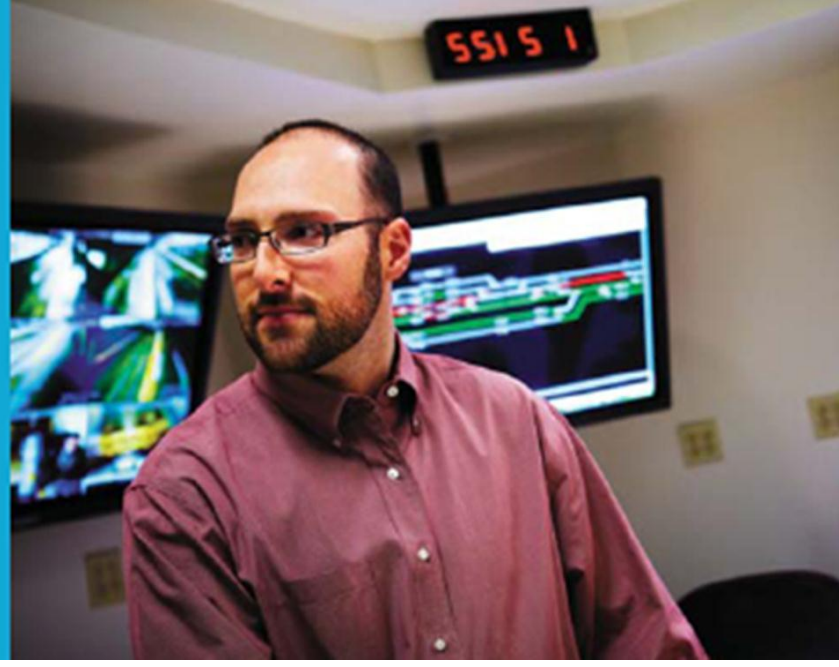
Windows Server 2012

创新，从云开始

通过动态访问控制掌控敏感数据



随着组织迁移到虚拟化程度越来越高的环境中，安全性这个概念有了全新的意义。您能确保只有经过授权的用户才可以访问机密数据吗？对审计访问有相应的粒度控制吗？事实上，安全性和访问控制对每个公司都是需要的。今天，在管理访问控制的方法上，组织还需要更大的灵活度。

动态访问控制是一种新的机制，它可以从组织级别集中定义访问策略。这些策略可以被自动地应用到每一个文件服务器，并作为一个总体的安全保护，与现有的共享和文件授权相结合。从本质上讲，动态访问控制通过在Active Directory用户和计算机增加“声明”属性，集成到 Windows 授权模式当中。如果您已经在使用Active Directory域服务，Windows Server 2012当中的动态访问控制功能，将会给您提供一个新的工具，供您控制数据的访问，并实现法规遵从。

轻松识别需要保护的文件

您能否识别组织中需要保护的文件？一个简单的事实是，很多组织并不知道它的企业中有什么样的信息（或者只是知道有很多文档）。这是 “标记”的用武之地，在“标记”这个过程会对文档的内容进行识别，然后根据逻辑定义对文档进行归类。在 Windows Server 2012当中，您可以采用一系列不同的方法对文档进行标记。例如，您可以通过添加文件到一个文件服务器的特定文件夹，以使用基于位置的标记；该文件接下来将会使用与父文件夹相同的标记。您还可以根据文件的内容自动标记文件。此外，用户和管理员还可以手动标记文件，或让动态访问控制功能通过API 扩展，支持第三方应用程序的标记方法。通过这一系列的实现方式，可为您提供更大的灵活度，并帮助您保证所有敏感信息都得到很好的保护，甚至您根本不知道存在的文件也是如此。

用于信息监管的中央访问控制

动态访问控制的核心理念是，访问应该被集中地进行控制。例如，组织可能需要限制只有文件所有者或人事部门成员才能够访问个人信息文档。或者，公司可能决定，如果要访问高度机密的数据，用户必须是全职的员工，并且必须使用一台受管理的设备，同时使用智能卡登录。

访问需要加以控制的原因有很多，而且这些限制很可能需要在整个组织层面或针对特定的用户和数据进行实施。所有这些访问策略都可以在Active Directory当中定义，非常容易管理。一旦定义完成，这些策略就可以通过组策略技术推送并应用到到一些（或全部）域内文件服务器上。，之后，使用动态访问控制对用户访问文件服务器上的分类数据进行评估。

让安全审计更简单更强大

安全审计是组织维持安全的最强大的工具之一，，这对于实现合规性是绝对必要的。但事实上，收集、存储和分析审计事件是非常昂贵和费时的。

Windows Server2012 的动态访问控制技术能够帮助您简化整个流程，让您在“声明”和资源属性的基础上建立审计策略，。例如，您可以审核没有高级别的安全授权，但是尝试访问高安全性敏感数据的用户；或者审计所有尝试访问与他们项目无关的文档的供应商。其结果是您可以有针对性的面对较少的重要事件。而且由于审计功能可以被很容易地扩展到第三方审计和监控平台，包括 Microsoft System Center Operation Manager，借此可简化整个组织的安全审计。

当访问被拒绝时，获得更好的修正

如果用户访问所需要的数据时被拒绝，您该怎么做？目前，沟通和解决问题是一个耗费时间的流程，IT 部门要承担这些工作任务，而同时，用户也无法具备他们所需的生产力。动态访问控制机制中包含了一些能够帮助这些用户自助解决相应问题的步骤。

该技术可以实现自我修正。动态访问控制提供了一个常规的拒绝访问消息，它是由服务器管理员为用户撰写的，以便用户能够在遇到拒绝访问的情况时进行自我修正。此消息还可以包含 URL，以便将用户定向到组织提供的自我修正网站。。

随后可以为数据所有者在被拒绝的情况下提供正确的访问权限，管理员可以以分发列表的形式来定义共享文件夹的所有者，这样用户就可以直接联系数据所有者来请求访问权限。这两种场景都可以降低对业务的整体影响。但即使是IT 管理员必须要进行干预，他们仍只需在这些问题上花费很少的时间，因为在进行干预的时候已经获取了足够多的问题细节。

根据文档分类自动地加密文档

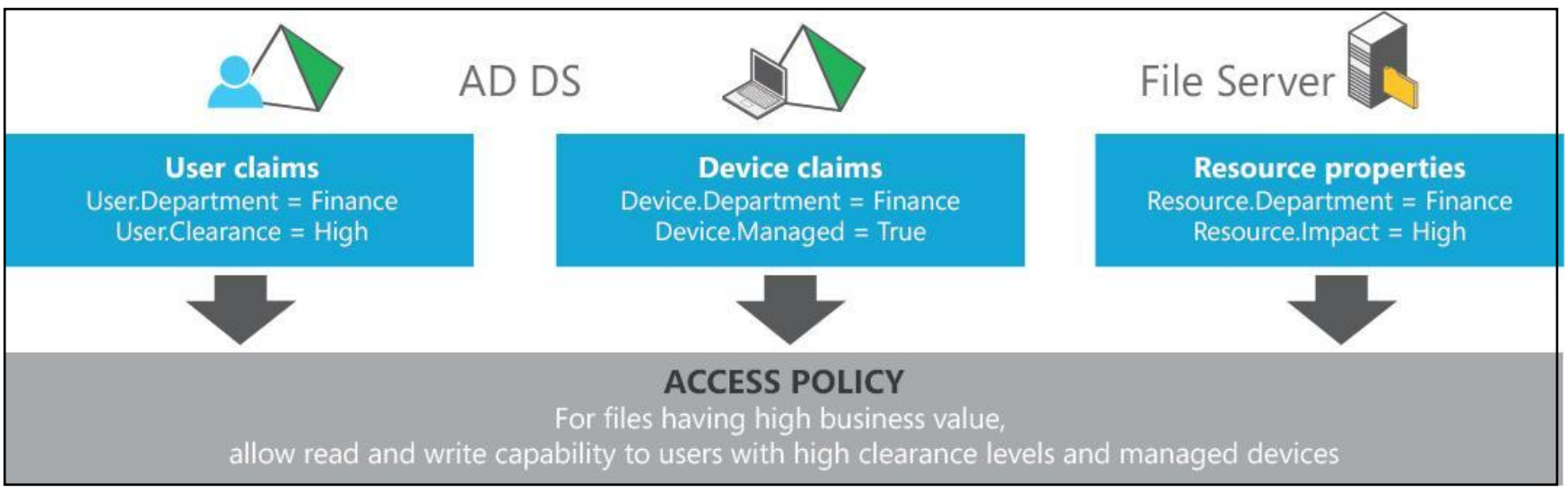
Active Directory权限管理服务（ADRMS）是一个很棒的、专门针对微软Office 文档进行加密的插件，该功能使得只有授权用户才能访问他们的内容，即使这些内容被意外地通过电子邮件消息的方式发送给了别人。Windows Server 2012的动态访问控制能够帮助简化加密流程，现在可以自动触发Active Directory权限管理服务，根据文档分类提供相应的保护。

例如，财务部门的用户可能创建了一个共享的文件，一旦该文件被确认为包含敏感信息，Active Directory权限管理服务将会将自动把该文件的访问权限限制在财务部门的用户中来进行保护。随后，任何试图访问该文档的用户必须首先获得Active Directory权限管理服务服务器的授权。只有用户是有效的财务部门的用户的情况下，文件才能打开。

时刻掌控您的敏感数据

不管是在本地服务器上，还是在云中，Windows Server 2012和动态访问控制机制都可提供新的安全标准和访问控制。通过 Windows Server 2012和动态访问控制，您将能够：

- 对于存储在您的组织的文件服务器上的内容获得更高的洞察力，并可以创建中央访问控制策略，快速、安全地保护所有数据。
- 通过实施特定的基于“声明”和文件归类的访问控制策略，提高您的灵活度。
- 花费更少的时间在收集、存储和分析安全审计事件上，而把更多的时间用在可能会导致合规性问题的有针对性的情况上。
- 当遇到拒绝访问问题是，授权用户和内容的所有者自助解决，从而减少对 IT 的影响。
- 通过动态访问控制策略自动地使用Active Directory权限管理服务插件加密文档，从而获得更高的安全性。



了解详情

想要了解更多关于Windows Server 2012能如何帮助您的信息？

请访问 http://www.microsoft.com/zh-cn/server-cloud