Windows Server 2012
创新，从云开始

通过 Dynamic Access Control 控制敏感数据

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？事实是，对安全和访问进行控制不单是一个很好的事情，对每个公司也是一个必须的要求。今天，在管理访问控制的方法上，组织需要更大的灵活度。

动态访问控制是一种新的机制，它可以定义组织级别的中央文件访问策略。这些策略可以被自动地应用到每一个文件服务器中，并作为一个总体的安全网，与现有的共享和文件授权相结合。从本质上讲，动态访问控制是将“申报”的理念 —— 即 Active Directory 用户和计算机属性 —— 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库，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基础架构中有什么样的信息（或者只是知道有很多文档）。这是发明“标记”这个概念的原因。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它的 API 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。

集中地控制访问权限

动态访问控制的核心理念是，访问可以，而且应该被集中地进行控制。例如，组织可能需要限制用户访问所有者或成员是 HR 部门的人所创建的，包含个人身份信息的文档。或者，公司可能决定，如果要访问有高影响力的数据，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，但所有这些在 Active Directory 当中定义的策略都易于管理。一旦定义完成，这些策略就可以通过组策略技术推送到任何（或全部）域文件服务器上。接下来，策略将会被应用到这些文件服务器上，针对使用动态访问控制进行分类的数据来评估相应的用户访问请求。

让安全审计更简单更强大

安全审计是其中一个最强大的工具，组织可以用它来维持安全，这对于实现合规性是绝对必要的。但事实是，收集、存储和分析审计事件可能非常昂贵和费时。

通过让您能够创建基于申报和资源属性的审计策略，Windows Server2012 中的动态访问控制技术能够帮助简化整个流程。例如，您可以审核所有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人；或者审计所有尝试访问与他们特定的项目无关文档的供应商。其结果是事件活动更少，因此您可以让活动更具针对性。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。

该技术可以自我修正。动态访问控制提供了一般的“拒绝访问”消息。这一消息是由服务器管理员撰写的，并能够为组织内的用户提供自助修正访问问题的连接。

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，管理员可以使用分布式的列表来定义共享用户，通过这些共享的用户，被拒绝的用户可以申请访问权限。这两种场景都可以降低对业务的整体影响。但即使是服务台或 IT 管理员必须要进行干预，他们仍只需在这些问题上花费较少的时间，因为在进行干预的时候已经获取了足够多的问题细节。

Microsoft

根据文档分类自动地加密文档

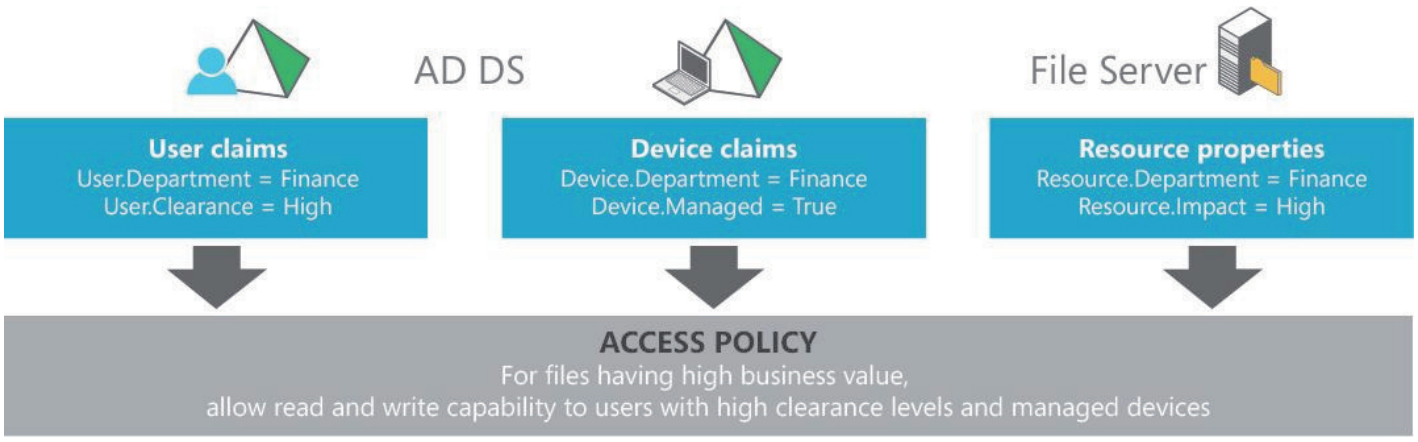
Active Directory 权限管理服务是一个很棒的，专门针对微软 Office 文档进行加密的插件，该功能使得只有授权用户才能访问他们的内容，即使这些内容被意外地通过电子邮件消息的方式发送给了别人。Windows Server 2012 的动态访问控制能够帮助简化加密流程，因为您现在可以自动化地触发 Active Directory 权限管理服务，根据内容的归类提供相应的保护。

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 权限管理服务保护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。随后，任何试图访问该文档的用户必须首先获得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

不管您是工作在本地服务器上，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 ：

- 对于存储在组织中文件服务器上的内容获得更大洞察力，并创建能够快速、安全地保护所有文件的集中式策略。
- 通过实施特定的基于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，花费更多的时间在有针对性的，可能会导致合规性问题的情况上。
- 通过允许用户和内容所有者自助解决访问拒绝的问题，降低对 IT 的影响。
- 通过使用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 如何帮助您的信息？请您访问 www.microsoft.com/windowsserver2012

Microsoft