Windows 服务器应用程序管理器

以基于角色的用户访问控制为 Windows 服务器保驾护航

Ivanti® Windows 服务器应用程序管理器可以限制那些需要登录服务器来执行特定工作任务的用户的管理权限，以便控制服务器访问并降低风险。当遇到拥有多个管理员用户的多功能服务器（如 SQL 和 IIS），或需要遵守 IT 基础架构安全实践相关规定的企业时，这种控制方法尤为有效。

通过 Windows 服务器应用程序管理器，IT 部门可将管理权限限定在特定的控制台、应用程序、服务和命令上。

用户只有在登录服务器后才能执行特定任务

通过 Ivanti Windows 服务器应用程序管理器，IT 部门可将管理权限限定在特定的控制台、应用程序、服务和命令上，从而降低管理员使用恶意软件、停止必要服务或影响关键任务服务性能的风险。

权限调整

向没经验的用户授予 IT 系统管理员的服务器完全管理权限会造成许多风险，比如错误地启动或停止服务、错误地安装或卸载软件等。这样会增加安全风险和管理成本、降低生产能力、产生法律和责任风险，且难以满足合规性。收回用户的完全管理权限，在用户处理特定工作任务时再提升用户相应权限，这样您就可以简化端点安全、减少支持呼叫量，并降低总体拥有成本 (TCO)。

应用程序管理器

Ivanti Windows 服务器应用程序管理器可根据应用程序白名单，允许授权访问服务器应用程序、服务和组件。IT 部门可使用应用程序管理器来为文件添加 SHA-1、SHA-256 或 ADLER32 数字签名，从而保证其完整性。

此外，IT 部门还能通过检查文件元数据（包括供应商、证书、发布者、版本等）来确保应用程序、组件和脚本的版本正确，阻止被修改过的应用程序或欺诈应用程序运行。

系统控制保护

通过系统控制将访问调整或限定至特定的服务，不但能防止服务器应用程序和流程被删除或修改，还能避免命名事件日志被清除。

应用程序黑名单

快速应用黑名单，控制管理员访问关键应用程序和服务器操作系统组件。黑名单可防止关键服务器资源被修改，并增强数据中心的服务器防护能力。

命令行限制

借助 Windows 服务器应用程序管理器，您可以将安全策略应用于执行应用程序及其相关命令行参数上。对于 Windows PowerShell 等服务器环境下的应用程序，您可以将管理员访问限定为加载特定的文件和脚本，或仅在特定条件下运行应用程序。

应用程序网络访问控制

这项功能无需路由器、交换机、防火墙等复杂工具即可阻止网络访问。它还能消除 IT 管理员在从特定服务器访问安全数据中心或网络资源时造成的安全漏洞。

情境控制

应用程序管理器可以根据登录用户的环境来实施大量条件检验，从而管理对服务器资源的访问。您可以根据条件（包括但不限于：用户、组或 OU 成员、设备名称、设备 IP 或 MAC 地址、连接客户端信息、操作系统、站点成员、日期和时间，甚至是使用 PowerShell、VBscript 或 Jscript 创建的自定义规则）评估环境。此外，Microsoft RDSH、Citrix XenApp、Citrix XenServer 和 Vmware 的全方位集成支持确保了安全策略同样能够应用到远程会话中。

www.ivanti.com.cn

010-85153668

IvantiChina@ivanti.com