【揭秘】AppLocker 工作原理！原来背后藏着这些秘密！

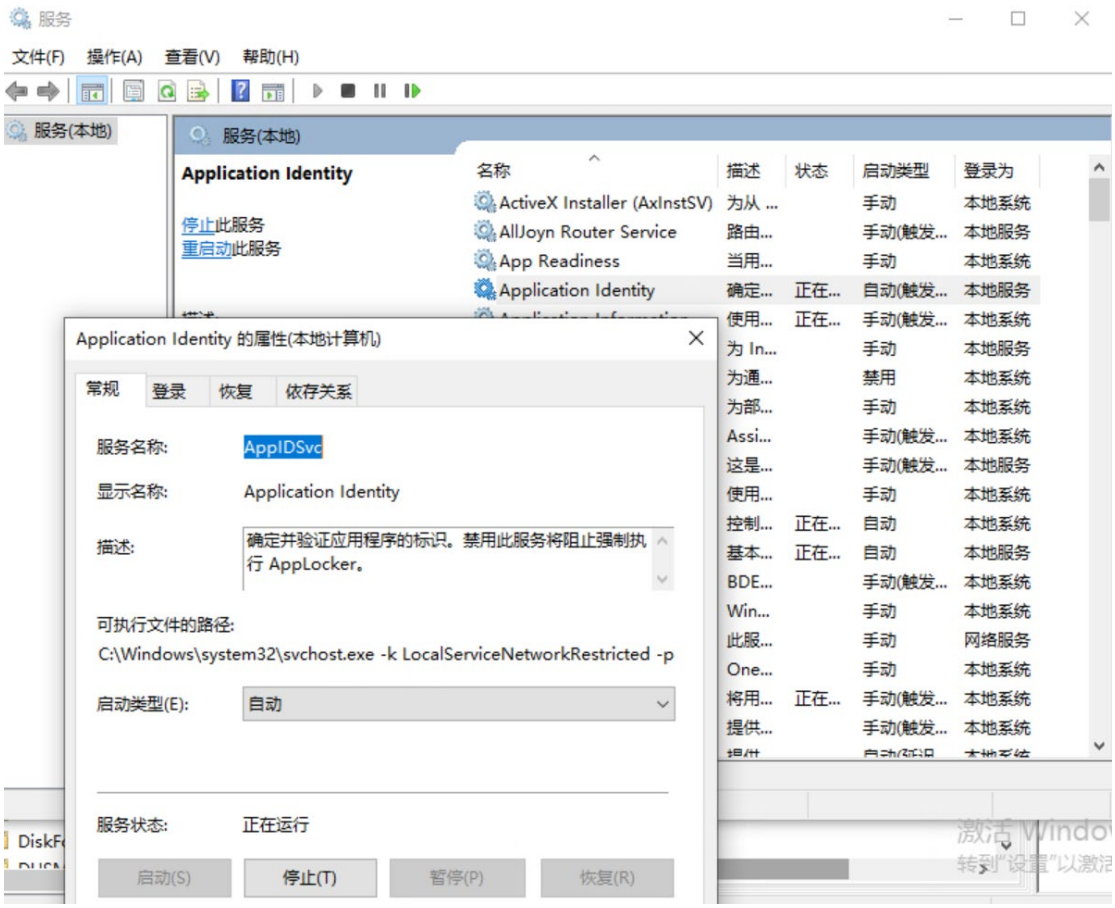
大家好！前两期给大家介绍了 Windows 操作系统中用于应用程序控制和安全策略的工具——AppLocker，并对比了 AppLocker 与软件限制策略（Software Restriction Policies，简称 SRP）的不同特点。

你可能会问，AppLocker 是怎么工作的呢？它怎么能如此聪明地保护我们的应用程序？别急，让我来告诉你！

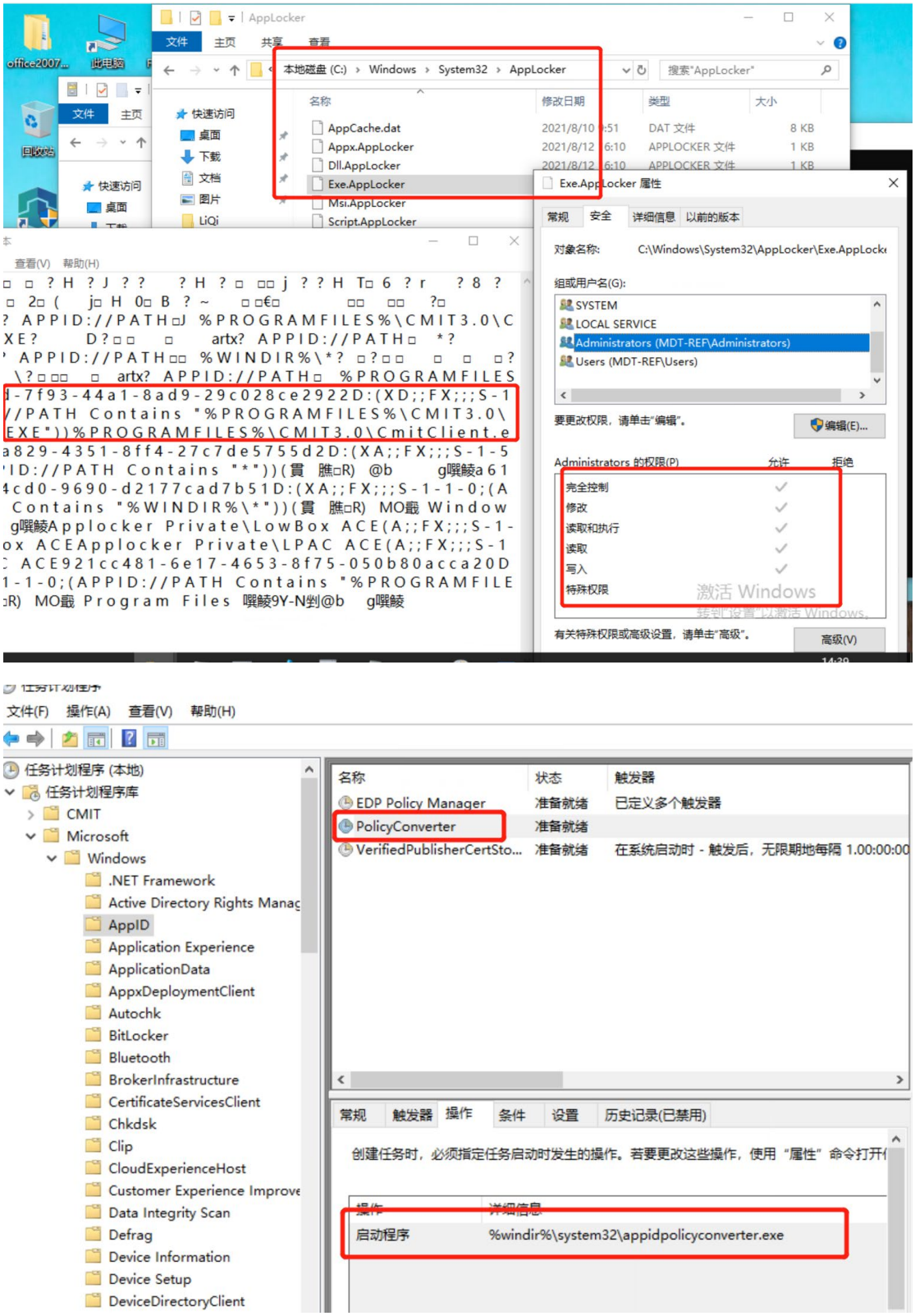
AppLocker 服务（AppIDSvc） 和 SRP 服务，其实是一对好兄弟，它们共存于同一个库（AppIdSvc.dll）中，并通过一个 SvcHost 进程运行。

该服务请求了注册表变动通知功能，就像一个超级警卫，时刻监视着注册表键值的改动。

而这些注册表键值，可以由 GPO 或本 ID 安全策略 MMC 管理单元中的 AppLocker 界面写入，也就是管理员设置的规则。

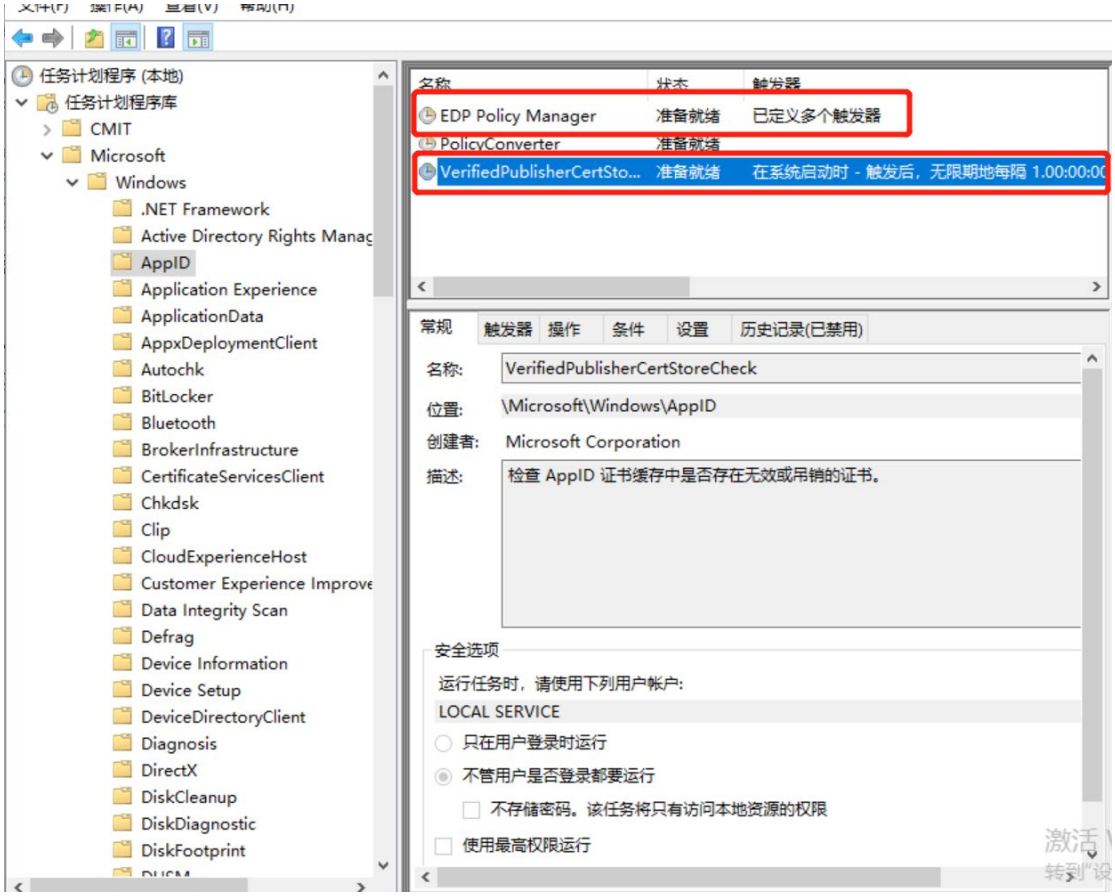


在检测到变化后，AppID 服务会触发一个用户模式任务（AppIDPolicyConverter.exe），该任务将读取（使用 XML 描述的）新规则，并将其转换为二进制格式的 ACE 和 SDDL 字符串，这样才能被用户模式和内核模式的 AppID 以及 Applocker 组件所理解。该任务会将转换后的规则存储在 HKLM\SYSTEM\CurrentControlSetlControl\Srp\Gp 键下。该文件只能由 System 和 Administrators 写入，对通过身份验证的其他用户是只读的。用户模式和内核模式的 AppID 组件会直接从注册表读取转后的规则。



另外 AppIDSvc 还会监视本地计算机的受信任根证书存储，并会通过一个用户模式的任务（AppIdCertStoreCheck.exe）验证这些证书，验证工作每天至少进行一次，或在证书存储出现变化后也会进行验证。AppID 内核模式驱动程序

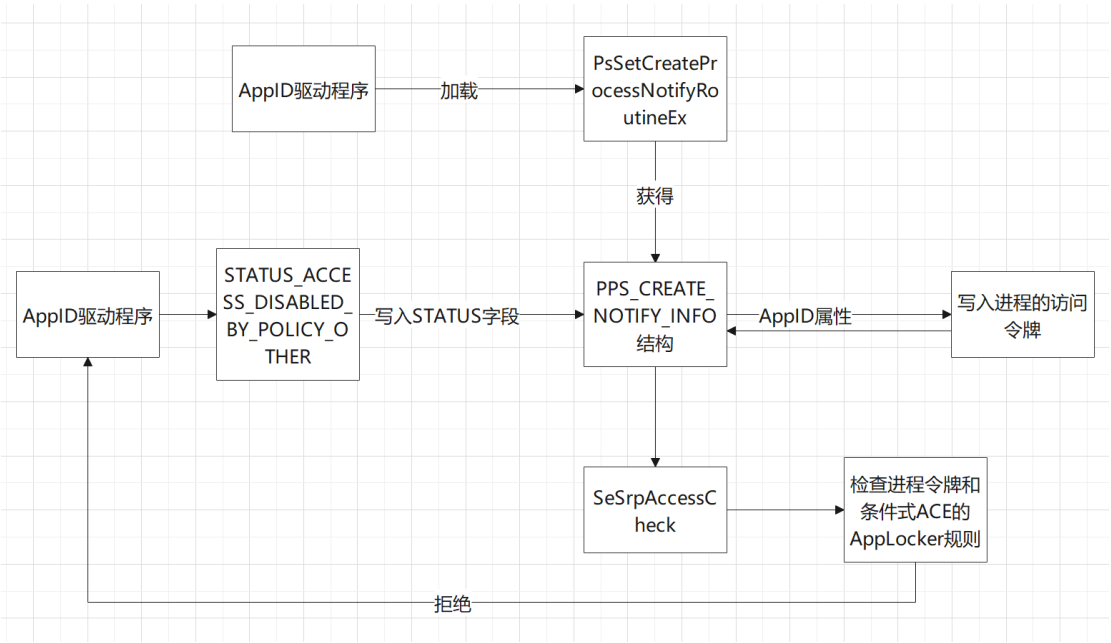
（%SystemRoot%\System32\drivers\AppId.sys）可以通过 APPIP_POLICY_CHANGED 这个 DeviceIoControl 请求接到 AppIDSvc 发来的有关规则出现变化的通知。



其中 AppID 服务使用 LocalService 账户运行，因此可以访问系统中的受信任根证书存储区域，也可以借助它来进行证书验证。AppID 服务则负责验证发行商的证书、将新证书加入缓存，以及检测 AppLocker 规则的更新并通知 AppID 驱动程序。

其中 AppID 驱动程序承担了 Applocker 的大部分功能，并依赖与 AppID 服务的通信（通过 DeviceIoControl 请求通信），因此其设备对象会受到 ACL 的保护，仅允许 NT SERVICE\AppIDSvc、LOCAL SERVICE 和 BUILTIN\Administrators 组访问。因而该驱动程序无法被恶意软件仿造。

当 AppID 驱动程序首先加载后，它会调用 PsSetCreateProcessNotifyRoutineEx 请求一个进程创建回调。当该通知例程被调用后，它会获得一个 PPS_CREATE_NOTIFY_INFO 结构（所创建进程的描述）。之后将已识别的 AppID 属性写入进程的访问令牌，接下来它会调用未文档化的 SeSrpAccessCheck 例程，由这个例程检查进程令牌和条件式 ACE 的 AppLocker 规则，进而确定进程是否允许运行。如果进程不允许运行，AppID 驱动程序会将 STATUS_ACCESS_DISABLED_BY_POLICY_OTHER 写入 PPS_CREATE_NOTIFY_INFO 结构的 Status 字段，这样即可导致进程创建操作被取消，并将设置进程的最终完成状态。对于 DLL，其限制方式为：映像加载器在将 DLL 载入进程时向 AppID 驱动程序发送 DeviceIoControl 请求。随后由 AppID 驱动程序针对 AppLocker 条件式 ACE 检查该 DLL 的标识。（对所要加载的每个 DLL 进行这样的检查会消耗大量时间，甚至会被最终用户察觉，因此 DLL 规则通常是禁用的。）



是不是觉得 AppLocker 工作原理很神奇？

AppLocker，就像是一个超级英雄，默默地保护着我们的应用程序，让我们的设备安全无忧！