nShield Container Option Pack

部署与高保障 nShield 硬件安全模块集成的容器化应用程序

精彩亮点

- 可让客户搭配使用 nShield 硬件安全模块来构建其容器化部署，以实现动态应用程序可扩展性，发挥硬件安全模块的最大功用
- 提供结构良好的容器化部署模型以及相关脚本，以创建应用程序容器映像
- 根据各种 Linux 平台基础模板创建映像
- 与经 FIPS 和 Common Criteria 认证的防篡改 nShield Connect 硬件集成，为业务关键型加密密钥提供高度安全的保护
- 可与 “nShield 即服务” 部署兼容

nShield Container Option Pack

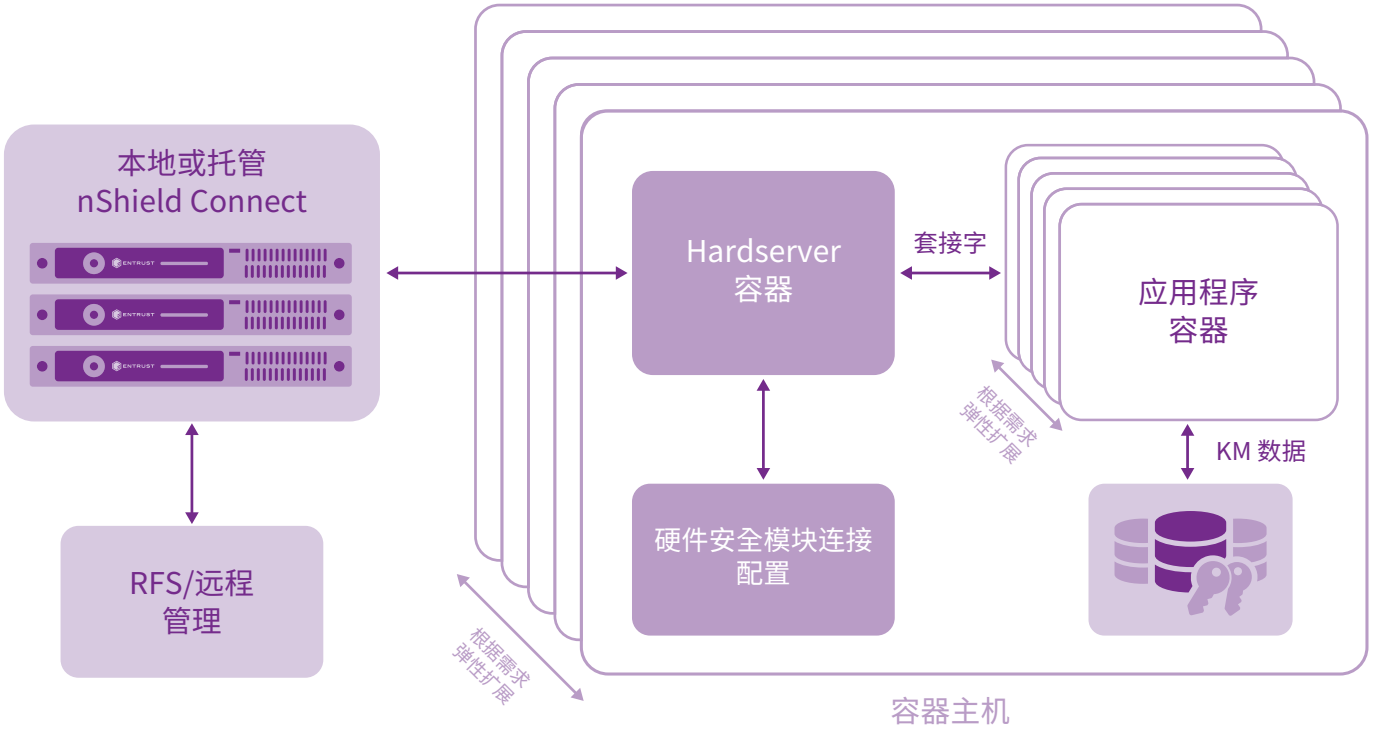
使用容器化应用程序的开发者可能不熟悉如何与高度安全的硬件安全模块 (HSM) 集成，并不清楚其中的复杂性。从筹划到生产阶段非常重要，您需要切实可靠的部署模型和脚本，帮助缩短整体开发周期。nShield Container Option Pack (nCOP) 可轻松为这些容器化解决方案提供 硬件安全模块支持，提供模板部署模型，让您着力于容器化应用程序，而无需担心 硬件安全模块集成。

nCOP 是 Entrust nShield 系列软件选项包的成员，旨在与我们的 nShield Connect 硬件安全模块默契协作，可以通过标准接口将硬件安全模块直接安全地集成到容器化应用程序。

nShield Container Option Pack

高级别架构

通过 nCOP，可以轻松访问灵活且可扩展的容器化架构，与现有 nShield 硬件安全模块和 Security World 环境交互操作。



RFS：远程文件系统 | KM 数据：密钥管理数据

图 1：nCOP 的高级别架构

nShield Container Option Pack

技术规格

操作系统支持	支持的硬件安全模块	可扩展性和许可证
• 仅限 Linux 版本	• 与所有 nShield Connect 硬件安全模块型号兼容 • 可与云托管的“nShield 即服务”硬件安全模块部署兼容	• nCOP 对 hardserver[1] 或应用程序容器没有强制的数量限制，可以与任意数量的容器主机（物理或虚拟服务器实例）配合使用。 • 与 nShield Connect 配合使用时需要用到客户端许可证，具体取决于部署规模。该选项包含了一个乘数，根据在运行的应用程序容器的最大部署数量来计算所需的客户端许可证数量。请参考图 2，获取各种部署规模所需的客户端许可证数量指南。

各硬件安全模块的客户端许可证数量	容器主机最大数量	允许的应用程序容器最大数量
5	5	50
10	10	100
15	15	150
20	20	200
>25	25	> 250 建议购买企业版客户端许可证

图 2：根据容器主机和应用程序容器规模，每个硬件安全模块所需的客户端许可证数量

注解 1：hardserver 是 nShield Security World 软件的守护程序服务组件，负责通过网络与 nShield 设备进行安全通信。PKCS#11 和 Java 库等客户端组件使用套接字与该进程结合。

进一步了解

如需进一步了解 Entrust nShield 硬件安全模块，请访问 **entrust.com/HSM**。如需进一步了解 Entrust 的身份、访问权限、通信和数据数字安全解决方案，请访问 **entrust.com**

如需进一步了解 Entrust nShield 硬件安全模块

HSMinfo@entrust.com
entrust.com/HSM

关于 ENTRUST CORPORATION

Entrust 支持受信任的身份、付款和数据保护，为世界的安全运转保驾护航。如今，无论是处理跨境业务、购买商品、访问电子政府服务还是登录公司网络，人们都比以往更加需要顺畅安全的体验。Entrust 提供了无与伦比的数字安全和凭证颁发解决方案，直接打通这些交互的核心。Entrust 在 150 多个国家/地区拥有 2,500 多位同事以及巨大的全球合作伙伴和客户网络，因而深受全球大多数托管组织的信任。

如需进一步了解，请访问：
entrust.com/HSM

ENTRUST

联系我们：
HSMinfo@entrust.com