

kaspersky

基本安装服务：

**Kaspersky Unified Monitoring
and Analysis Platform**

简介

卡巴斯基专家服务涵盖产品生命周期的各个阶段，提供从评估、实现到维护和优化等一系列服务。

卡巴斯基 SIEM (Kaspersky Unified Monitoring and Analysis Platform) 是新一代解决方案，旨在帮助您的安全团队管理和分析传入的安全数据。它的优势在于：

- 收集、处理和存储各种来源的事件，包括卡巴斯基解决方案、操作系统、第三方应用程序、安全工具和数据库；
- 实时分析和关联传入数据，并利用业界领先的威胁情报对其进行增强，从而检测可疑活动；
- 提供及时的警报，以便快速进行事故调查和响应；
- 通过热存储和冷存储选项以及无缝的同步搜索功能，在不超出昂贵存储硬件预算的情况下，长期存储数据。

通过将 Kaspersky Unified Monitoring and Analysis Platform（以下简称 KUMA）与其他产品和系统集成，可以提高威胁监控和响应的效率，并扩展保护范围。

本文档介绍了 Kaspersky Unified Monitoring and Analysis Platform 服务的基本安装和配置流程及阶段。该服务由卡巴斯基技术支持团队提供。

此服务的目标是在约定的工作范围内，在您的环境中部署并运行 KUMA。

服务范围

一台 KUMA 服务器，连接最多 10 个事件源，与最多 3 个卡巴斯基解决方案或基础架构服务集成。

服务时间表

此服务最多需要 10 个工作日内来完成目标。若全部内容交付完毕且您验收满意，即使实际工作日不足 10 日，项目也将被视为“完成”。

服务可分为以下几个阶段：

- 启动会议、检查清单填写和范围确认
- 规模计算
- 部署和基本配置
- 事件源连接
- 实现后工作

要求及其他信息

请注意，如未完全满足以下列出的要求，卡巴斯基没有义务提供或尝试提供此服务。

此服务以远程方式交付。为了准备和提供部署方案，您需要提供卡巴斯基工程师要求的数据。

在服务交付期间，贵公司 IT 部门或安全团队的代表必须始终在岗，以满足卡巴斯基工程师提出的任何合理要求，包括权限、访问等。

此服务基于当前受支持的 KUMA 版本提供，并遵循应用程序生命周期期限：

(<https://support.kaspersky.com/corporate/lifecycle?type=limited,full&program=kuma>)

部署过程中出现的任何技术问题将通过我们的支持服务进行解决。

工作范围

1. 规模计算（收到客户问卷后开展）
2. 部署：
 - 2.1. 根据规模计算验证硬件需求（CPU/RAM、磁盘）
 - 2.2. 验证服务器之间的网络连接
 - 2.3. 配置 DNS 客户端和 NTP 客户端
 - 2.4. 准备操作系统（SSH 密钥设置、sshd 配置、按需创建逻辑卷和挂载点）
 - 2.5. 在服务器上分发安装包（使用 kuma-ansible-installer）
 - 2.6. 激活授权许可
 - 2.7. 安装存储集群
 - 2.8. 安装收集器微服务（针对预定义的标准源）
 - 2.9. 安装关联器微服务
3. 与基础架构服务集成
 - 3.1. 配置域身份验证 (FreeIPA / Active Directory)
 - 3.2. 为 AD 组分配特定角色权限
 - 3.3. 与 LDAP 服务器集成（一台服务器）
 - 3.4. 与 SMTP 服务器集成
 - 3.5. 配置从卡巴斯基存储库直接更新（如果可直接访问互联网；不包括 KUU 的额外部署和配置）
4. 实现后工作：知识转移和总结报告

成果和交付物

完成 KUMA 的部署和配置，您的管理员将了解如何部署 KUMA 并完成基本配置。您将收到一份完成报告。

备注



我们可以通过定制化的专业服务组合，执行超出我们现有服务包范围的额外配置、部署以及其他多项任务。请联系您的客户经理，讨论如何为您定制专属方案。

此类服务的示例包括：

- 事件源集成，包括标准事件源
- 非标准事件源的自定义解析器开发
- 检测（关联）规则的调优和开发
- 各种响应操作的配置
- 自定义报告

我们的工作安排将根据卡巴斯基适配资源的可用情况而定，但开始时间不晚于收到您书面项目启动批准后的 15 天内。



www.kaspersky.com.cn

© 2026 AO Kaspersky Lab。

保留所有权利。注册商标和服务标志均为其各自拥有者的财产。