

89Kubernetes 系列（八十三）提升：发现用于高级安全性和可观察性的合规 Kubernetes 解决方案

在 Kubernetes 中实现 GDPR 和 ISO 27001 合规性：生产工作负载的基本技巧

介绍

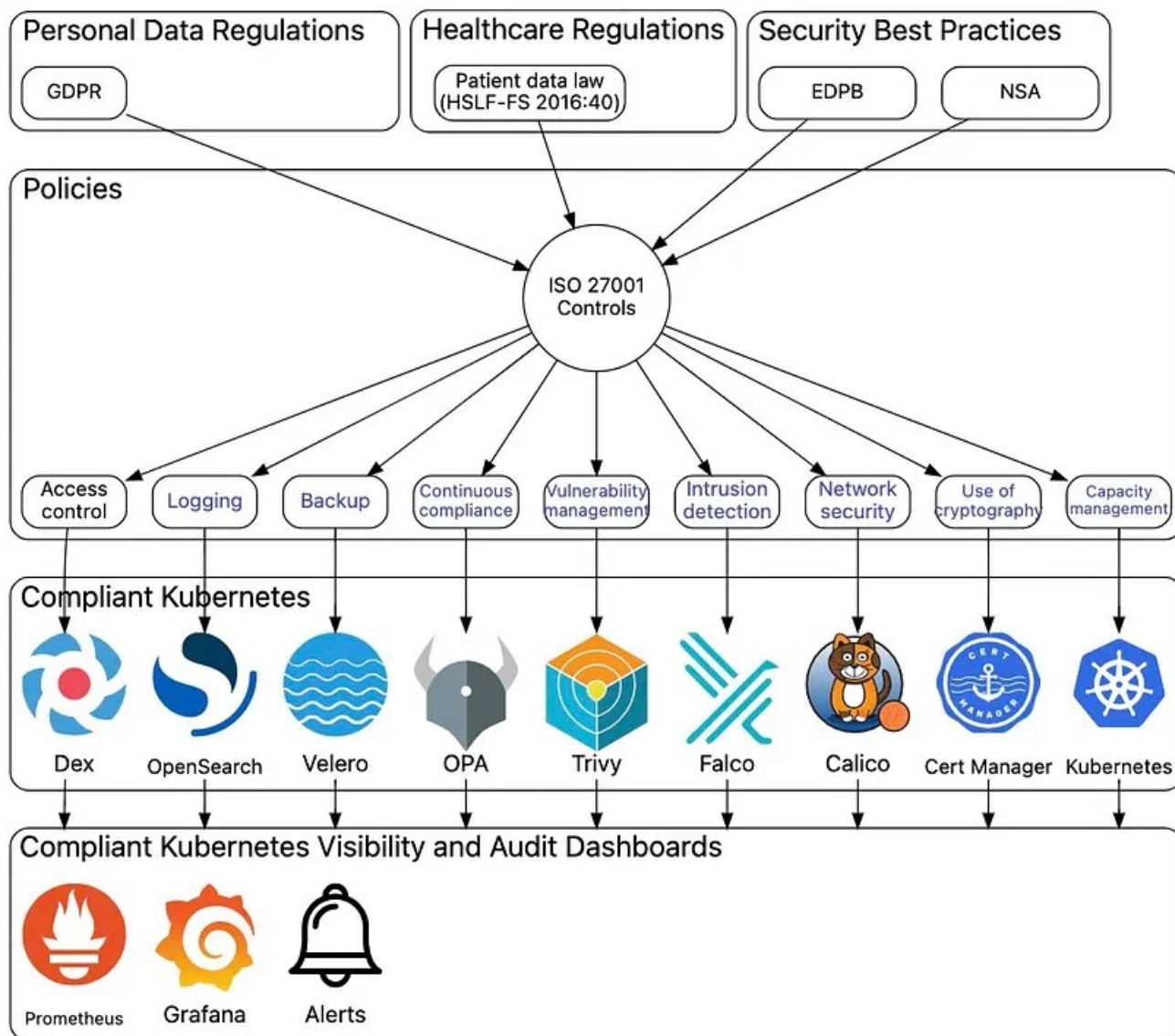
随着公司越来越多地利用 Kubernetes 来运行生产工作负载，确保遵守数据保护法规和信息安全标准变得至关重要。

在 Kubernetes 环境中实现 GDPR 和 ISO 27001 合规性需要一种全面的方法来解决各种安全问题。

目标：

从实施入侵检测系统和策略即代码框架到容器镜像扫描和网络分段，这些技巧为增强安全性、保护个人数据和满足监管要求奠定了基础。

快乐学习📖



<https://elastisys.io/compliantkubernetes/>

Created by elastisys

以下是针对在 Kubernetes 上运行生产工作负载并且必须满足 GDPR 和 ISO-27001 合规性要求的公司的一些建议。

实施入侵检测系统：??

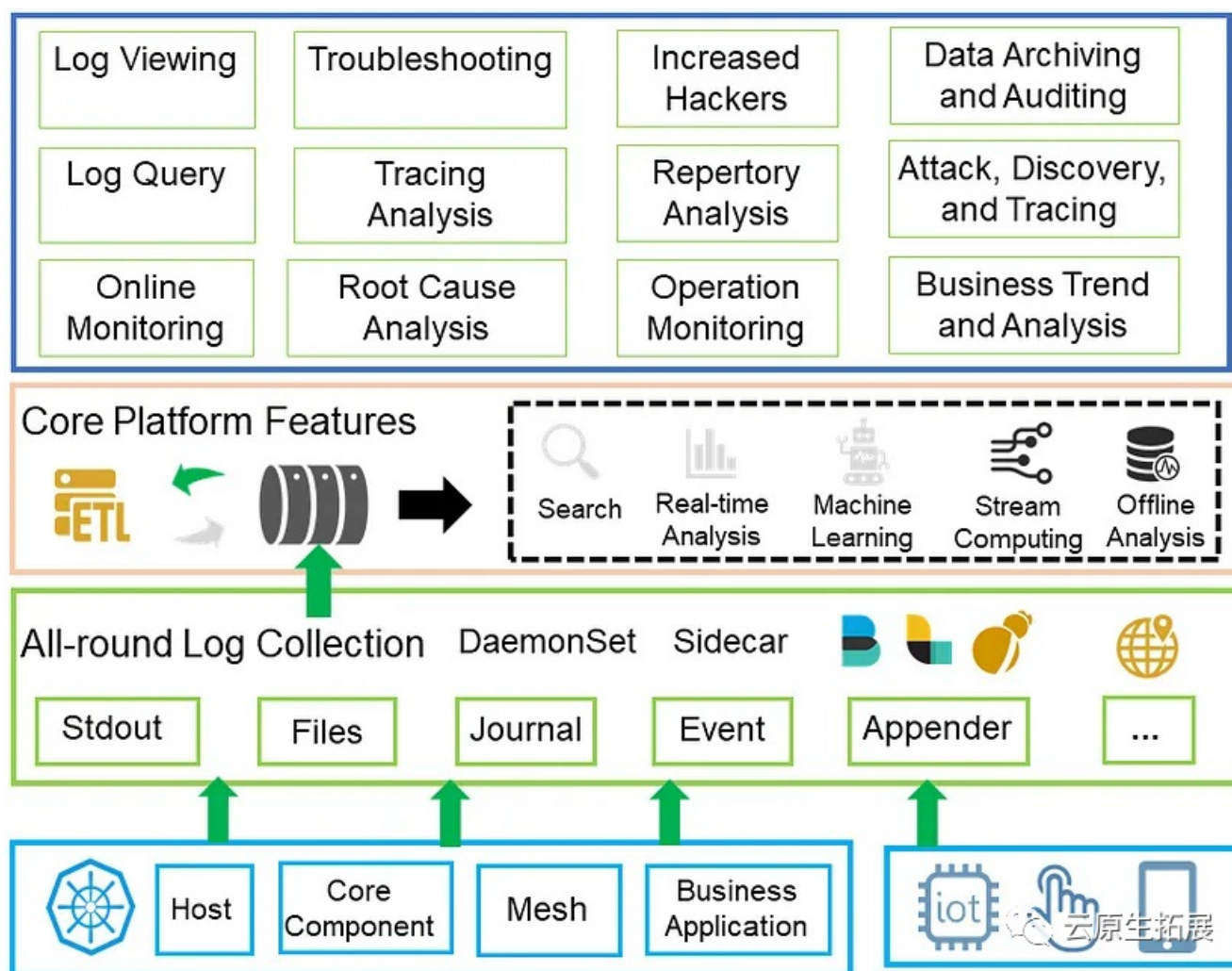
入侵检测系统可以帮助监控和识别 Kubernetes 环境中潜在的安全漏洞或恶意活动。通过部署像 Falco 这样的工具，您可以检测可疑行为或未经授权的访问尝试并发出警报。这对于满足 GDPR Article 32 要求和 ISO controls A.12.2.1, A.12.6.1, and A.16.1.7 很重要。



正确配置警报并建立处理它们的流程：🔗

正确配置安全系统（包括入侵检测系统）生成的警报至关重要。

定义根据特定事件或模式触发警报的阈值和规则。为您的运营团队建立一个流程，以便及时处理这些警报、调查潜在的安全事件并采取适当的措施来降低任何风险。



使用策略即代码（例如，OPA/Gatekeeper）：🔗

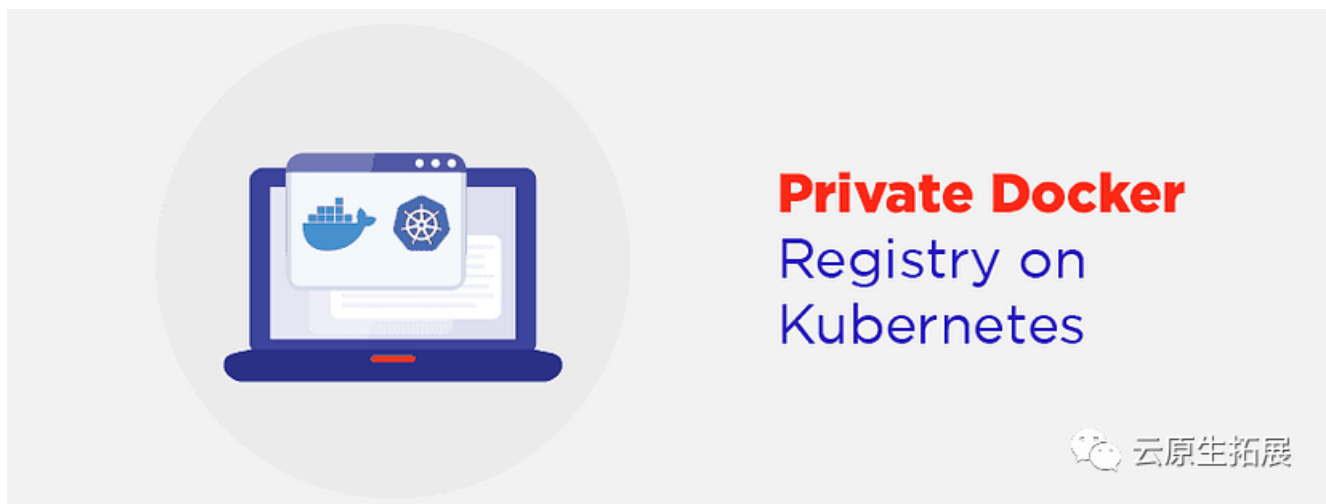
Open Policy Agent (OPA) Gatekeeper 和 Kyverno 等策略即代码工具允许您为 Kubernetes 部署定义和执行策略。通过编纂组

织的安全策略，您可以防止微不足道的错误配置并实施最佳实践。这与 ISO controls A.18.2.2 和 A.18.2.3 相关，它有助于保持对特定安全要求的遵守。



设置具有漏洞扫描功能的私有仓库（例如 Harbor）：

部署像 Harbor 这样的私有仓库可以让您控制容器镜像并确保它们符合安全标准。通过集成 Trivy 和 Starboard 等漏洞扫描工具，您可以持续扫描容器镜像以查找已知漏洞。这有助于解决 GDPR Article 32 要求和 ISO control A.12.6.1，确保您部署安全且可信的容器镜像。



使用分段工具实施网络策略：

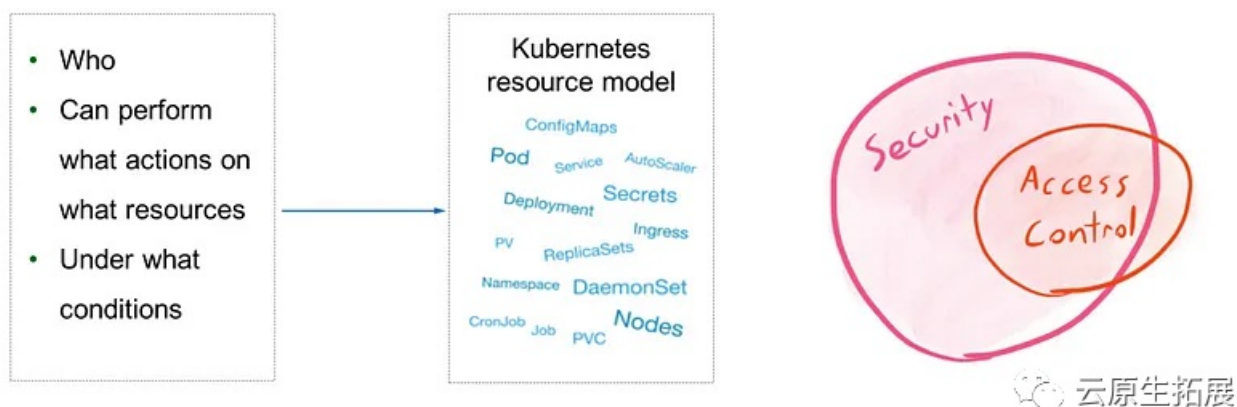
使用 Calico 等工具实施 NetworkPolicies 有助于通过启用网络分段来提高 Kubernetes 集群的安全性。NetworkPolicies 允许您定义细化规则来控制集群中不同组件和命名空间之间的网络流量。这可以在发生安全漏洞时限制爆炸半径，有助于满足 ISO control 1.13.1.1-3。

数据加密：

实施加密机制可确保敏感数据同时受到 **at rest** 和 **in transit** 的保护。利用 **Secrets** 和 **ConfigMaps** 等 **Kubernetes** 功能来安全地管理加密密钥和其他敏感信息。加密对于 **GDPR** 合规性至关重要，有助于满足与数据保护相关的 **ISO** 安全控制。

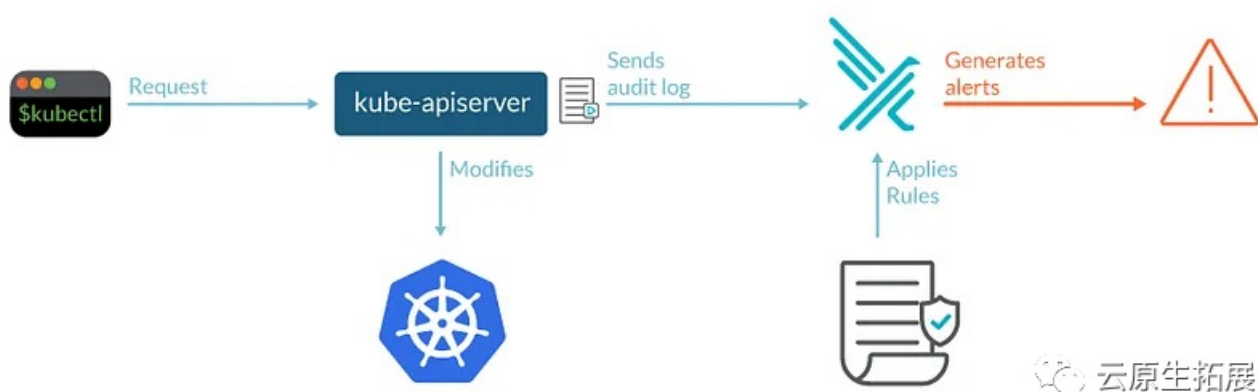
访问控制和 RBAC:

适当的访问控制对于确保只有授权的个人在您的 **Kubernetes** 环境中拥有必要的权限至关重要。利用 **Kubernetes RBAC** 根据最小权限原则为用户和服务帐户分配角色和职责。这有助于满足 **ISO control** 的要求，并且是 **GDPR compliance** 的一个重要方面。



日志和审计: ②

在 **Kubernetes** 集群中启用全面的日志记录和审计功能，以监控和跟踪活动和事件。从各种组件收集日志并将它们集中起来，以便于分析和关联。定期查看日志以识别任何异常、安全事件或策略违规。这对于满足 **ISO control** 要求和证明符合 **GDPR Article 32** 是必不可少的。



定期安全补丁和更新:



























使用最新的安全补丁使您的 **Kubernetes** 集群和相关组件保持最新状态对于维护安全环境至关重要。定期测试和部署更新以解决任何已知漏洞并确保您的集群免受潜在威胁。这有助于满足与安全和风险管理相关的 **GDPR** 和 **ISO** 要求。

灾难恢复和备份: ②

制定全面的灾难恢复计划以确保 **Kubernetes** 工作负载的可用性和完整性。定期备份关键数据，确保备份数据加密存储安

全。

Components of Elastisys Compliant Kubernetes

Additional Services	 PostgreSQL	 Redis	 RabbitMQ	 TimescaleDB	 Harbor	 ArgoCD (preview)	 Jaeger (preview)
Security	 Gatekeeper	 Starboard	 Dex	 falco	 Kured	 Trivy	
Logs	 fluentd	 OpenSearch		 Grafana	 Prometheus	 Thanos	 AlertManager
Disaster Recovery	 Velero	 Rclone					
Kubernetes	 Kubernetes	 containerd	 Terraform	 Kubespray	 Helm		

Created by 云原生实践

总结

有了正确的范围、正确的警报文化和正确的维护，您应该有能力维护 Kubernetes 平台的稳定性和安全性，以应对所有“已知的知识”。我们还讨论了如何通过限制性网络策略、入侵检测和日志审查来加强您的 Kubernetes 平台的安全性，以应对“已知的未知数”和“未知的未知数”。