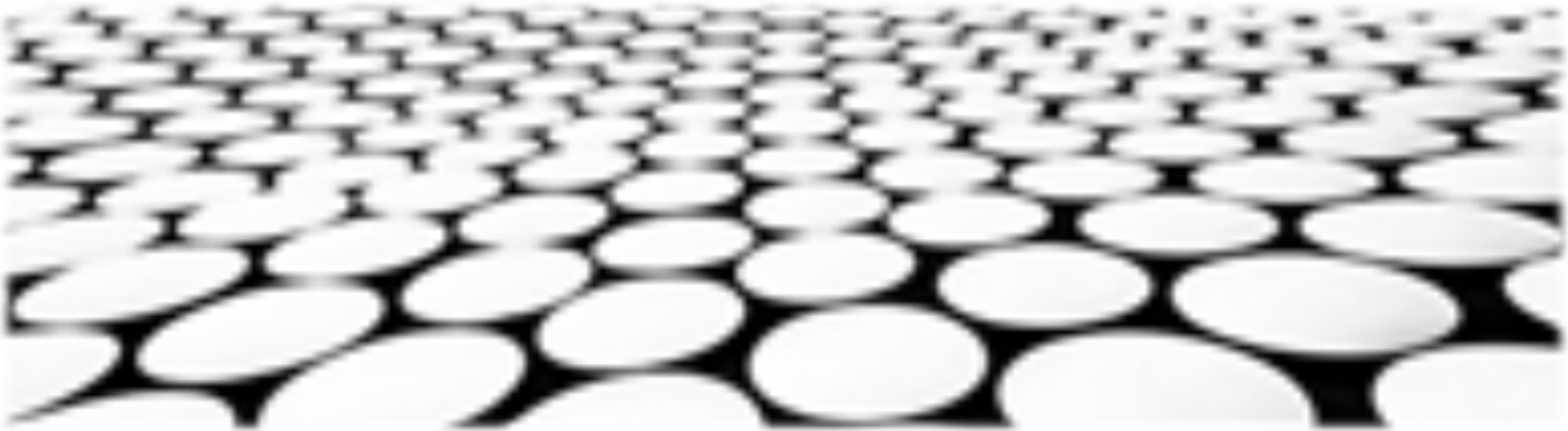
数智创新 变革未来

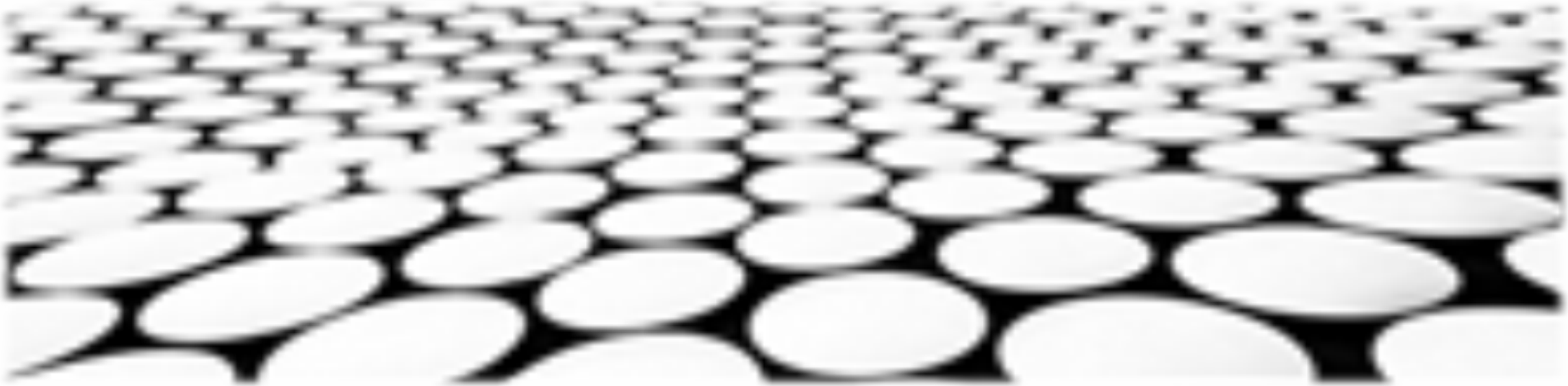
容器化进程隔离



目录页

Contents Page

Linux 内核命名空间



Linux 内核命名空间

Linux内核命名空间

1. 进程隔离：命名空间将进程隔离到不同的容器中，每个容器具有自己独立的网络栈、文件系统和资源限制。
2. 资源管理：命名空间允许管理员在容器之间精细地分配资源，确保每个容器仅使用其所需资源。
3. 安全增强：命名空间隔离不同容器的进程，防止恶意或受感染的进程访问其他容器中的资源。

进程间通信

1. 共享内存：命名空间支持共享内存段，允许容器之间的进程高效地共享数据。
2. IPC 机制：命名空间提供进程间通信 (IPC) 机制，例如管道、FIFOs 和信号。
3. 控制资源：管理员可以配置命名空间的 IPC 机制，以控制容器之间的通信方式。

Linux 内核命名空间

文件系统隔离

1. 私有文件系统：每个命名空间都有自己私有的文件系统，使容器能够独立管理自己的文件和数据。
2. 挂载点：容器可以挂载外部文件系统作为自己的私有文件系统的子目录。
3. 文件访问控制：命名空间允许管理员实施文件访问控制，以限制容器对文件系统的访问。

网络隔离

1. 独立网络栈：每个命名空间具有自己的独立网络栈，包括网络接口、IP 地址和路由表。
2. 网络策略：管理员可以配置网络策略，以控制容器之间的网络通信。
3. 网络边界：命名空间可以创建网络边界，以隔离容器免受外部网络威胁。

Linux 内核命名空间

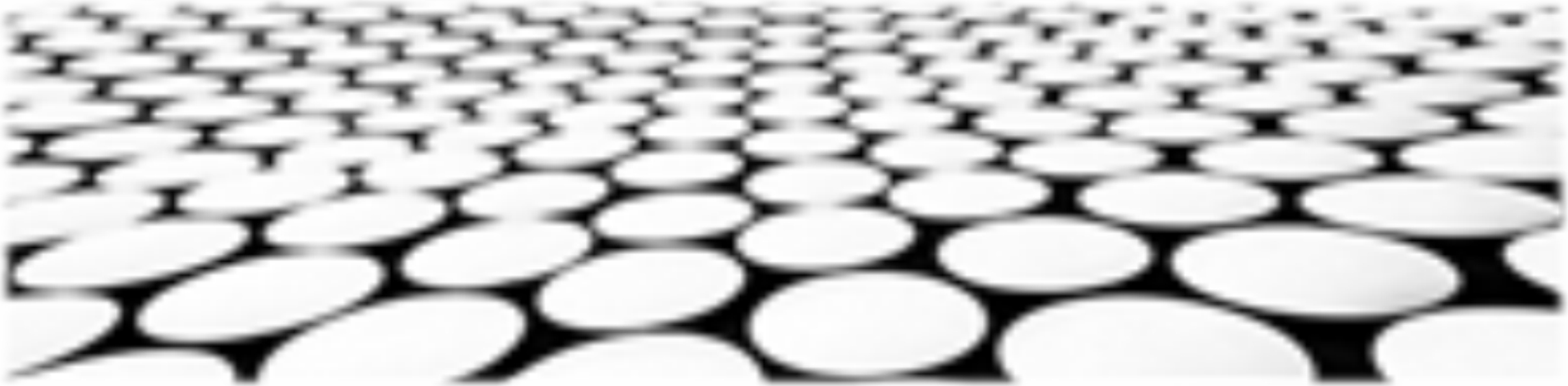
资源限制

1. CPU 和内存限制：命名空间可以对分配给容器的 CPU 和内存等资源设置限制。
2. I/O 限制：命名空间可以限制容器的 I/O 操作，以防止它们耗尽系统资源。
3. 自定义资源限制：管理员可以创建自定义资源限制，以满足特定应用程序的需求。

安全沙箱

1. 进程隔离：命名空间创建了一个安全沙箱，将容器中的进程隔离在自己的命名空间内。
2. 特权能力限制：命名空间限制容器中的进程获得特权能力，例如访问底层硬件。

用户与组命名空间



用户与组命名空间

用户命名空间

1. 隔离用户标识信息：在用户命名空间中，容器内运行的进程拥有与宿主机不同的用户和组标识符，从而防止容器内进程访问敏感的用户文件和权限。

2. 实现权限最小化：通过隔离用户命名空间，可以将容器的权限限制到最小所需，降低容器逃逸和权限提升的风险。

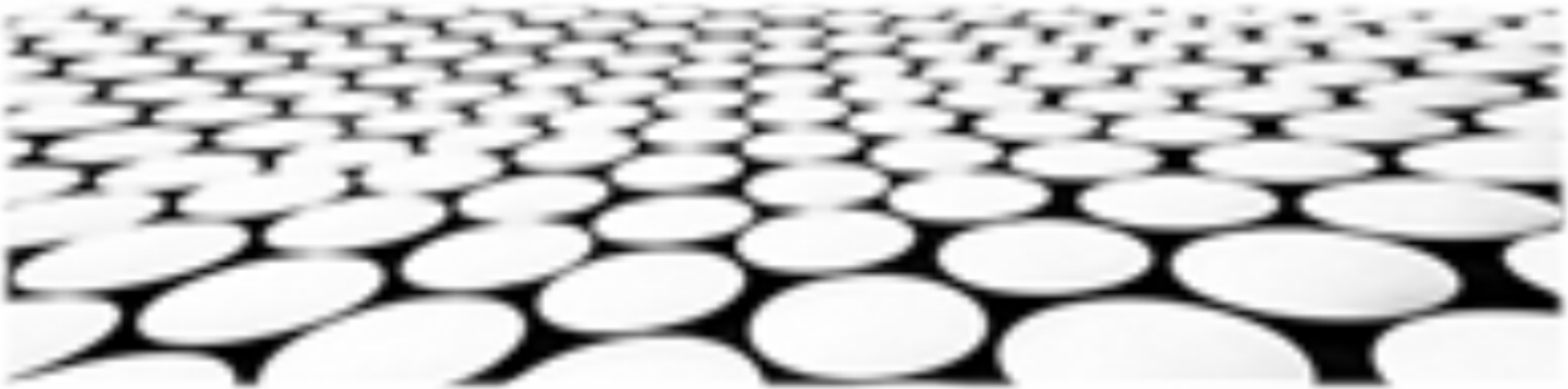
3. 增强安全边界：隔离的用户命名空间为容器提供额外的安全边界，限制恶意代码或进程从容器内传播到宿主机或其他容器。

组命名空间

1. 隔离组成员关系：类似于用户命名空间，组命名空间隔离了容器内的组成员关系，防止容器内进程获取敏感组权限。

2. 防止特权提升：通过隔离组命名空间，可以防止容器内进程通过获取特权组权限来提升其权限。

网络命名空间



网络命名空间

网络命名空间：

1. 隔离网络栈：网络命名空间提供一个隔离的网络环境，使每个容器拥有自己的 IP 地址、路由表和端口号，从而实现进程之间的网络隔离。

2. 自定义网络设置：容器可以通过网络命名空间自定义其网络设置，如 IP 地址分配、网关配置和防火墙规则。这种灵活性增强了容器的网络控制和安全。

3. 网络策略实施：网络命名空间与网络策略（如网络策略和安全组）相结合，可以为容器实施精细化的网络访问控制。

基于VLAN的网络隔离：

1. 物理隔离：基于 VLAN 的网络隔离在物理网络层隔离容器流量。每个容器分配一个专用 VLAN，确保数据在不同容器之间物理隔离。

2. 网络性能提高：与网络命名空间隔离相比，基于 VLAN 的隔离提供了更低的延迟和更高的吞吐量，因为流量不再受限于软件定义的边界。

3. 硬件支持：基于 VLAN 的隔离需要网络交换机或虚拟交换机提供硬件支持。这可以降低软件开销，并提高网络性能。

网络命名空间

Overlay网络隔离：

1. 逻辑隔离：Overlay 网络通过在底层物理网络之上创建逻辑隧道来隔离容器流量。允许不同主机上的容器在同一个逻辑网络中通信。
2. 跨主机通信：Overlay 网络使容器能够跨多个物理主机进行透明通信，从而增强了应用程序的可扩展性和容错能力。
3. 服务发现和负载均衡：Overlay 网络通常集成服务发现和负载均衡机制，简化了容器之间的通信和资源管理。

基于组播的网络隔离：

1. 多播网络：基于组播的网络隔离使用多播网络技术将流量发送到特定组成员。仅允许加入该组的容器接收该流量，从而实现细粒度的网络控制。
2. 安全性和可扩展性：组播隔离提高了安全性和可扩展性，因为流量仅发送给目标组，减少了网络拥塞和广播风暴。
3. 动态组成员资格：容器可以动态地加入或离开组，使网络隔离更容易适应应用程序的变更和扩展。

网络命名空间

容器网络接口（CNI）：

1. 可插拔的网络管理：CNI 提供了一个可插拔的接口，用于将容器连接到底层网络。它允许管理员在不同网络提供商或技术之间无缝切换。
2. 标准化配置：CNI 规范化了容器网络配置，简化了跨不同平台和环境的容器部署。
3. 生态系统支持：CNI 拥有一个不断增长的生态系统，其中包括各种网络插件和工具，为容器网络提供灵活性、可扩展性和安全性。

vSphere7的虚拟分布式交换机（vDS）：

1. 集中式网络管理：vDS 提供了一个集中式平台来管理虚拟网络，包括容器网络。它简化了网络配置、故障排除和性能优化。
2. 高级安全性：vDS 内置高级安全功能，如分布式防火墙和入侵检测系统，为容器网络提供保护。

挂载命名空间