

SAN 加密具有硬件独立性并简化了密钥管理，因而可降低成本并提高灵活性。不再要求部署特定的自加密驱动器。Virtual SAN 加密还支持双因素身份验证 (SecurID 和 CAC)，因而能够很好地保证合规性。另外，它还是首个采用 DISA 标准的 STIG 的 HCI 解决方案。

- 支持单播网络连接，以帮助简化初始 Virtual SAN 设置。可以为 Virtual SAN 网络连接使用单播，不再需要设置多播。这使得 Virtual SAN 可以在更广泛的本地和云环境中部署而无须更改网络。
- 优化的数据服务进一步扩大了 Virtual SAN 的性能优势。具体而言，与以前的 Virtual SAN 版本相比，它可将每台全闪存主机的 IOPS 提升 50% 之多。提升的性能有助于加快关键任务应用的速度，并提供更高的工作负载整合率。
- 借助对最新闪存技术的现成支持，客户可加快新硬件的采用。此外，Virtual SAN 现在还提供更多的缓存驱动器选择（包括 1.6TB 闪存），方便客户使用更大容量的最新闪存。
- 经验证的全新体系结构为部署 Splunk、Big Data 和 Citrix 等新一代应用提供了一条行之有效的途径。此外，Photon Platform 1.1 中提供了适用于 Photon 的 Virtual SAN，而新的 Docker Volume Driver 则提供了对多租户、基于策略的管理、快照和克隆的支持。
- 借助新增的永不停机保护功能，Virtual SAN 可确保用户的应用正常运行和使用，而不会受潜在的硬件问题的影响。新的降级设备处理功能可智能地监控驱动器的运行状况，并在发生故障前主动撤出数据。新的智能驱动器重建和部分重建功能可在硬件发生故障时恢复更快，并降低集群流量以提高性能。

7. Virtual SAN 6.7

Virtual SAN 6.7 为第七代 Virtual SAN，VMware vSphere 6.7 可以说是为了 Virtual SAN 6.7 而发布的，可见 Virtual SAN 6.7 产品的重要性。其主要新增功能如下。

- 全新的引导式集群创建和扩展 workflow 提供了全面的向导，可协助管理员完成初始和后续运维。此 workflow 可确保所有步骤均按正确的顺序完成，让管理员胸有成竹地构建集群，包括延伸集群。
- VUM 可让管理员针对整个集群执行一致的生命周期管理。此次更新实现了 DELL、Fujitsu、SuperMicro 和 Lenovo 等大厂 vSAN ReadyNode 主机 I/O 控制器固件和驱动程序修补的自动化。运行状况检查可提醒客户有可用的新补丁程序。VUM 可为 HCI 集群提供自动化的补丁程序管理，还可管理计算和存储固件。
- 智能维护模式可在维护操作期间确保一致的应用性能和恢复能力。Virtual SAN 会提醒用户，进入维护模式的主机会影响性能；如果预测维护不会成功，还能主动将其停止，从而提供一定的防护。
- Virtual SAN 的 UI 中添加了新的高级集群设置，并在其 Power CLI 中添加了一些新的 cmdlet 命令。此外，在更换 vCenter Server 或从故障中恢复 vCenter Server 等场景中，Virtual SAN 可自动备份和恢复 SPBM 策略。
- UNMAP 可自动执行空间回收，减少了应用所用的容量。Virtual SAN 与客户机操作系统发起的 SCSI UNMAP 请求相集成，可在删除或截断客户机操作系统文件后