



Netwrix/Stealthbits Fpolicy最佳实践和建议

https://kb-cn-stage.netapp.com/on-prem/ontap/da/NAS/NAS-KBs/Netwrix_Stealthbits_Fpolicy_Best_Pr...

Updated: Wed, 22 Apr 2026 12:46:01 GMT

适用场景

- ONTAP 9
- CIFS
- NFS
- Netwrix
- Stealthbits
- FPolicy

问题解答

与Netwrix Fpolicy部署相关的最佳实践和建议有哪些？

- 本指南对于确保您同时了解Netwrix和NetApp端最佳实践至关重要。
- [适用于Netwrix活动监视器的NetApp Fpolicy部署最佳实践](#)

'NetApp provides no representations or warranties regarding the accuracy or reliability or serviceability of any information or recommendations provided in this publication or with respect to any results that may be obtained by the use of the information or observance of any recommendations provided herein. The information in this document is distributed AS IS and the use of this information or the implementation of any recommendations or techniques herein is a customers responsibility and depends on the customers ability to evaluate and integrate them into the customers operational environment. This document and the information

Netrix的具体建议：

这些建议将根据Netrix准则一起执行、可能需要客户联系Netrix以获取更多详细信息或说明。

- 根据Netrix准则、确保Netrix版本为最新版本、包括此Hotrix的增强功能(SAM_6.0_029)
 - 客户必须直接与Netrix支持部门联系、才能获取有关此修补程序的详细信息。
 - 此处附加了一份修补程序信息副本SAM_6.0_029 (有关最新信息、请与Netrix联系)
 - 新版本将更好地处理突发活动事件、并针对改进的事件处理和其他增强功能进行了优化。
 - 请联系Netrix以确保您获得最佳版本。
- 其他Netrix专用最佳实践
 - 考虑使用多个主服务器进行横向扩展和容错。
 - 在ONTAP和活动监视程序代理之间使用低延迟链路。例如、活动监控代理应与受监控的NetApp设备位于同一数据中心。
 - 缩小监控范围(监控哪些操作、共享、卷)。建议不要监控已加载服务器上的目录读取操作。
 - 确保每个ONTAP集群节点的每个SVM都有一个LIF以连接到代理。

NetApp特定建议：

- 升级到具有已知fpolicy相关问题修复程序的适当ONTAP版本
 - [1438207 - 如果FPolicy进入限制状态、则它可能会停止向外部引擎发送屏幕请求](#)
- 对于Netrix外部引擎、将发送缓冲区大小设置为7895160
 - Netrix最佳实践是将设置为最大值："The FPolicy Send-Buffer Size is set to 7895160"

```
vserver fpolicy policy external-engine modify -vserver <vserver> -engine-name <engine-name> send-buffer-size 7895160
```

 - 有关如何设置send-buffer size的详细信息：
 - [如何计算ONTAP 9 FPolicy的发送缓冲区](#)
 - [在EMS和Fpolicy.log中发现写入EAGAIN错误](#)
- 要减少延迟的潜在影响、请在Netrix指导下将中止超时设置为较低值、例如：10s。
 - 如果代理和SVM之间存在大量延迟、则它可以对TCP加密延迟执行发生原因操作、并在极少数情况下对延迟产生潜在影响。

- 要在代理出现连接问题或CPU不足的情况下减少最终用户延迟、建议将"中止请求超时"从40秒降低到10秒：

```
vserver fpolicy policy external-engine modify -vserver <vserver -engine-name <engine-name> -reqs-abort-timeout 10s
```

- 请参见以下文档：[vserver fpolicy policy外部引擎命令- vserver fpolicy policy外部引擎show](#)。

一般建议：

- 根据[TR-4696](#)《Netwrix/Stealthbits最佳实践》

Expand All

7.5 管理FPolicy工作流程和对其他技术的依赖

NetApp建议在在进行任何配置更改之前禁用FPolicy策略。例如、如果要在为已启用策略配置的外部引擎中添加或修改某个IP地址、请先禁用该策略。

如果将FPolicy配置为监控NetApp FlexCache® 卷、NetApp建议您不要将FPolicy配置为监控 读取 和 getATTR 文件操作。要在ONTAP中监控这些操作、需要检索索引节点

到

路径(i2P)数据。由于无法从FlexCache 卷检索I2P数据、因此必须从初始卷检索这些数据。因此、监控这些操作会消除

FlexCache可提供的性能优势。

当同时

部署FPolicy和机下防病毒(AV)解决方案时、AV解决方案会首先收到通知。FPolicy处理 仅在AV扫描完成后开始。速度较慢的AV扫描器可能会影响整体性能，因此AV解决方案的大小必须适当。

定义范围时、将

要监控或审核的所有共享添加到共享/包含列表中。

如果不想

监视 共享，请关闭文件服务器上的monitoring。在SVM上禁用FPolicy

没有任何帮助，因为 Netwrix Activity Monitor 活动 代理 会定期检查 文件服务器

，如果没有断开连接 (如果 选择了“启用并连接FPolicy”

选项)，则会自动禁用或启用FPolicy。

7.6 大小设置注意事项

FPolicy对CIFS操作执行实时监控、向 外部服务器发送通知并等待响应、具体取决于外部引擎通信模式(同步或

异步)。此过程会影响CIFS访问和CPU资源的性能。

要缓解

任何问题、NetApp建议在启用FPolicy之前对环境进行评估和规模估算。

性能受用户数量、工作负载特征(例如每个用户的操作数、数据大小和网络延迟)的影响。

8 Netwrix文件活动监视器最佳Practices.

在将 Netwrix 文件活动监视器与NetApp文件服务器结合使用时，建议遵循以下最佳实践：

将 FPolicy配置限制为特定的卷、共享 和 操作，以减少对SVM的影响。

- 考虑部署多个 Netwrix活动监视器 活动 代理、以实现负载均衡和 容错。
 - 使用启用并连接FPolicy选项使SVM保持连接、并始终将 事件发送到 Netwrix 活动监视器 代理活动
-

追加信息

- [Varonis Fpolicy最佳实践和建议](#)
- [Veritas Fpolicy最佳实践和建议](#)
- [Komprise Fpolicy最佳实践和建议](#)
- [Cloud Secure Fpolicy最佳实践和建议](#)
- [Netwrix/Stealthbits Fpolicy最佳实践和建议](#)
- [什么是适用于ONTAP的FPolicy合作伙伴解决方案？](#)