Cisco Threat Grid 设备数据保留说明

首次发布日期: 2017 年 3 月 3 日

上次修改日期: 2020 年 6 月 23 日

数据保留信息

不同文件和数据类型的数据保留

文件/数据类型	每日数量	每日规模占用限制	保存时间	所需空间
分析	10,000	429.7 MB	至少 1000 天	464.1 GB
磁盘工件 (Blob)	150,000	16.6 GB	至少 4.3 天	76.5 GB
目录	10,000	39.1 MB	至少 64 天	2.6 GB
网络	10,000	4.5 GB	至少 64 天	311.1 GB
进程	10,000	1.0 GB	至少 64 天	71.2 GB
报告	10,000	1.3 GB	至少 1000 天	1.4 TB
样本	10,000	7.6 GB	至少 64 天	524.7 GB
Sandcastle-工作线程	10,000	39.1 MB	至少 64 天	2.6 GB
屏幕截图	10,000	468.8 MB	至少 4 天	2.0 GB
状态	10,000	39.1 MB	至少 4 天	168.8 MB
时间表	10,000	351.6 MB	至少 4 天	1.5 GB
USB 内容	10,000	39.1 MB	至少 64 天	2.6 GB
视频	10,000	5.0 GB	至少 64 天	345.5 GB
电话簿	10,300	270000 个文件中 37.3 GB/天	--	3.1 TB

其他数据保留信息

- 保留时间假定采样率为每日 10k。

- 在迄今未发布的 10k 样本设备上，至少将分析报告保留两年；在 TG5500s/TG5504s 上是上述时间的两倍；在 TG5000s/TG5500s 上比后者长 3 倍以上（即比 TG5500 保留期长 3 倍）。换句话说，比未发布的 10k 样本设备保留期长 6 倍以上。
- 分析数据适用相同的保留规则。
- 其他内容将保留较短的时间，具体取决于磁盘的可用性。
- 如果您运行的系统低于容量，则会保留更多内容并且保留更长时间。
- 2.2 迁移中将包含从系统位于 1.x 上开始的磁盘工件 (Blob)。
- 在 2.2 迁移后，Blob 只会保留较短时间。
- 由于一个样本可能有多个 Blob，因此 150,000 个 Blob/天的采样率代表平均值。如果您的采样率不同，可能会影响保留期。

严格实施保留期限制

在 2.6 版本中提供了一个 tgsh 配置选项，它不会将来自分析的工件存储十五 (15) 天以上，从而严格实施保留期限制。设置之后，在第一次夜间修建期间，将删除已超过 15 天的文件。

注：这一 15 天期间无法配置或更改。

工件是指样本本身以及从它们中生成的其他内容。工件不包括分析报告 HTML，后者适用另行用文档说明的其他原限制。项目也不包括数据库条目和搜索索引。

该 tgsh 选项为 **strict_retention**，默认处于禁用 (false) 状态。

要在 15 天后启用工件硬修剪，请在 tgsh 中将此选项设置为 true：configure set **strict_retention true**。