SecCenter ESM-AV-G 终端安全管理系统（防病毒） 隔离文件如何恢复

AV防病毒 卢鹏 2024-06-30 发表

问题描述

现场使用SecCenter ESM-AV-G 终端安全管理系统（防病毒）将正常文件报毒隔离，咨询 隔离文件如何恢复

过程分析

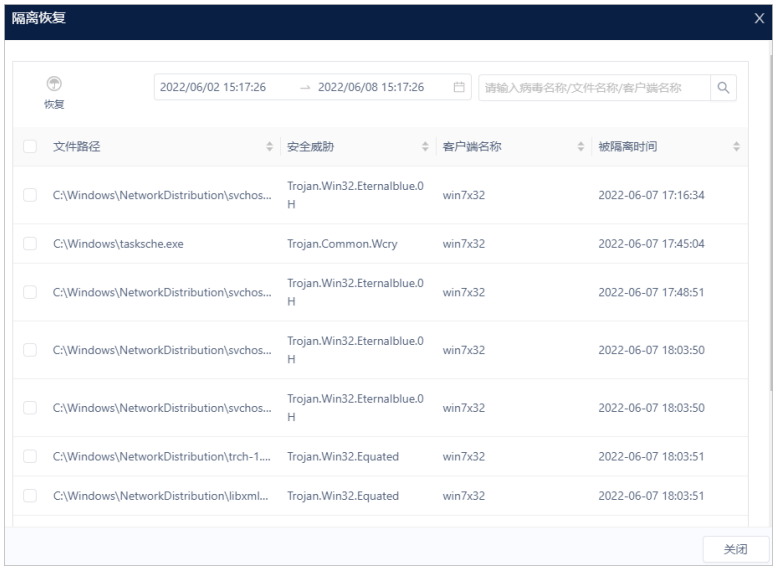
如果您认为检测不准确，则可以恢复终端安全管理系统防病毒隔离的文件。

(1) 转到“客户端 > 客户端管理”。

(2) 选中一个或多个客户端，单击<隔离恢复>。

(3) 弹出隔离恢复列表，列表中展示被这些客户端隔离的文件。

图3-14 隔离恢复列表



(4) 选择需要恢复的文件，单击<恢复>。

服务端向客户端下发隔离恢复任务，客户端收到隔离恢复任务后，将恢复指定的被隔离文件，并加入到客户端的扫描例外列表中。

解决方法

扫描例外

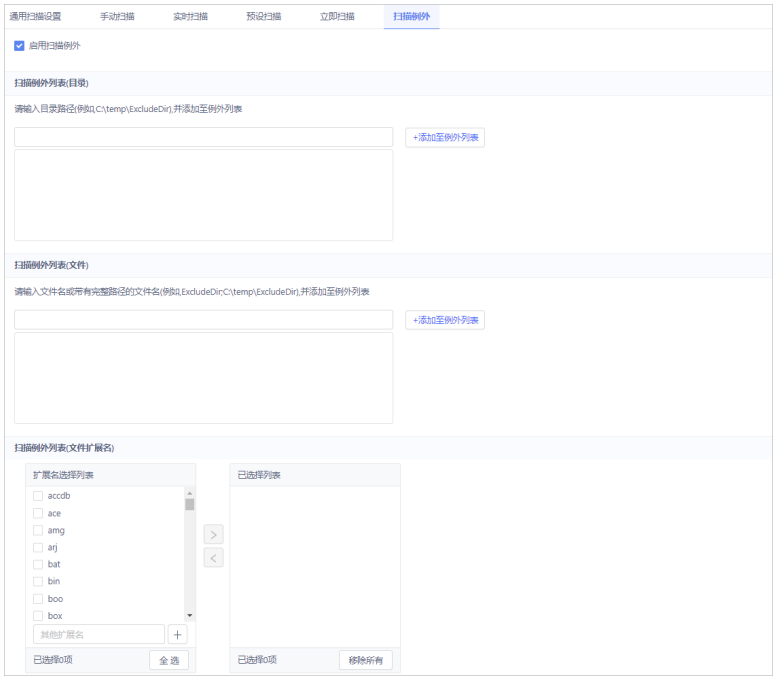
配置扫描例外可提高扫描性能并跳过对导致假警报的文件的扫描。运行特定扫描类型时，终端安全管理系统防病毒检查扫描例外列表，以确定终端上的哪些文件将从扫描中排除。扫描例外设置将应用至所有扫描类型。

启用扫描例外时，终端安全管理系统防病毒在以下情况下将不扫描文件：

- 文件位于特定目录（或其任意子目录）下。
- 文件名与例外列表中的任何名称匹配。
- 文件扩展名与例外列表中的任何扩展名匹配。

(1) 转到“防病毒规则 > 扫描例外”。

图5-11 扫描例外



(2) 配置以下内容：

- 启用扫描例外
- 扫描例外列表(目录)

  终端安全管理系统防病毒不扫描在计算机特定目录下找到的所有文件。从扫描中排除某个目录时，终端安全管理系统防病毒将自动从扫描中排除该目录的所有子目录。
- 扫描例外列表(文件)

  如果一个文件的文件名与此例外列表中包括的任何名称匹配，则终端安全管理系统防病毒将不扫描该文件。如果要排除在终端上特定位置找到的文件，请包括文件路径。
- 扫描例外列表(文件扩展名)

  如果一个文件的文件扩展名与此例外列表中包括的任何扩展名匹配，则终端安全管理系统防病毒将不扫描该文件。

另外，可以单击右上方的<导入>，导入例外列表。

图5-12 导入例外列表

单击<导出>，导出例外列表。如下图所示，导出的为策略名称为policy的扫描例外列表。

图5-13 导出例外列表

(3) 单击<保存>。