SecPath A2000-AK605(二代) 操作审计日志保存时长、大小以及能否修改

堡垒机 刘诚 2021-11-30 发表

组网及说明

不涉及

问题描述

堡垒机有操作审计功能，支持图形操作、字符操作等回放功能，这种日志保存的时长是多长？或者说占用存储空间的多少就会覆盖，能否对保存时长和占用存储空间大小进行修改？

支持图形、字符、文件传输、数据库操作审计
图形操作 审计记录回放，可在审计回放界面上，同步显示关键的键盘操作、标题栏操作、剪贴板操作等文字信息，并能在点击任意文字信息，可直面；
图形操作 审计记录回放，支持web、离线两种模式查看相应审计记录
图形操作 审计记录回放，支持倍速播放、定点取证功能
图形操作 审计记录回放，支持审计回放键盘同步功能
图形操作审计：文本审计，可以对图形操作过程中的键盘鼠标操作、剪贴板操作、标题栏事件进行文本审计
图形操作审计：会话缩略图，支持按会话大小自定义会话缩略图，通过定期生成的缩略图定位回放用户操作
图形操作审计：会话切片，支持图形会话审计记录支持会话切片管理功能
图形操作 审计检索，支持以键盘输入内容、剪贴板内容为关键字进行图形搜索，搜索结果可以直接定位到相关图形画面进行回放
图形操作 审计检索，支持以窗口标题为关键字进行检索定位
图形操作 审计检索，支持以URL链接为关键字进行检索定位
字符操作 审计记录回放，支持以录像方式完整展示用户的指令操作，同时支持命令输入、输出分屏管理
字符操作 审计检索，针对字符会话审计记录支持以输入、输出为关键字进行检索定位，搜索结果中关键字高亮显示，支持从任意命令处进行操作回放
文件传输审计，可以完整记录用户通过系统进行的文件传输操作（包括sftp、剪切板、RDP磁盘映射等），并可对传输的文件信息进行留存
数据库操作审计，支持sqlserver、mysql、oracle等数据库操作行为审计，可通过录像及sql语句方式查看用户相关操作
操作热点分析，以topN模型展示用户的操作热点，如高危指令热度、用户操作热度分析等
支持资源、用户、操作三个维度审计智能检索，包括多关键字检索、自定义检索标签、审计会话合并等功能

过程分析

13.1.19 定期任务：配置审计数据清理

运维审计系统支持每天在指定时间清理N天前的审计日志。

系统挂载点/var目录主要被审计数据占用。系统管理员请及时清理审计数据以确保该目录未被占满。当/var目录不足5GB时，所有访问资产的在线会话都将会断开，且无法启动任何新的会话。运维审计系统将在/var目录使用率超过80%和不足5GB时，分别在页面上方进行告警提示。

清理的审计日志包括：

- 字符会话、图形会话和数据库会话的操作审计日志。
- 文件传输日志，如果留痕还包括传输的文件（对于使用网盘模式传输的文件，如果文件被其他用户使用则不删除）。
- 登录日志。
- 配置日志。
- 审计记录。

Note: 运维审计系统不清理在线会话的审计日志。

审计数据清理支持以下两种方式：

- 定期清理：在指定时间执行清理任务，清理指定日期之前的数据。默认不开启。
- 自动清理：在审计数据的磁盘占用率达到指定的百分比后执行清理任务，清理现存日期最早的审计数据，直到系统目录的磁盘占用降到阈值以下。默认开启，默认清理阈值为80%。

13.1.19.1 配置定期清理

1. 选择系统设置 > 系统 > 定期任务 > 审计数据清理。
2. 选择启用，开启审计数据清理。
3. 设置定期清理时间（时和分）和天数（清理多少天以前的审计日志），完成后单击确定。

- 假设在2018年9月17日10:00执行清理任务，如果清理1天前的日志，那么清理的是9月17日00:00之前的日志；如果清理2天前的日志，那么清理的是9月16日00:00之前的日志。
- 清理审计日志时，以会话的开始时间判断审计日志是否符合清理条件。

Note: 如果要禁用该功能，可以先选中禁用，或者单击重置，然后单击确定。

配置完成后，运维审计系统每天在指定的时间清理N天之前的审计数据。审计日志清理定期任务执行后，上次执行时间将显示上次执行清理任务的时间和执行结果（包括失败原因）。审计管理员也可以在工作台 > 审计 > 事件审计 > 配置日志中查看到一条日志。

审计数据清理如果失败，所有超级管理员都将在右上角收到清理失败提醒。

13.1.19.2 配置自动清理

1. 选择系统设置 > 系统 > 定期任务 > 审计数据清理。
2. 勾选磁盘占用达到XX时自动删除现存最早日期的审计数据。
3. 设置自动清理的阈值。

取值范围为60%-90%，默认为80%。

如启用了自动清理，在Tomcat启动后，10分钟后将执行执行一次磁盘检查，后续将每隔4小时再执行一次检查。当检查到运维审计系统的系统目录（主要是审计数据）的磁盘占用达到该阈值时，将会清理审计数据。执行清理时会从现存日期最早的审计数据开始清理，直到系统目录的磁盘占用降到阈值以下。

Note: 对于在线会话的审计日志和网盘文件不会进行自动清理。如这两种文件占用空间已超过了设置的阈值，将会清除所有可以清理的审计数据。请用户自行保证不清理的文件占用的空间不会过大。

解决方法

审计数据清理支持以下两种方式：

- 定期清理：在指定时间执行清理任务，清理指定日期之前的数据。默认不开启。
- 自动清理：在审计数据的磁盘占用率达到指定的百分比后执行清理任务，清理现存日期最早的审计数据，直到系统各审计磁盘占用降到阈值以下。默认开启，默认清理阈值为80%。

14.6 如何备份审计日志?

审计日志包括字符和图形会话日志。

1. **超级管理员可以在系统设置中选择系统 > 定期任务 > 审计数据备份。**
2. **选择备份时间点和文件服务器。**

   运维审计系统会在该时间点，将前一天产生的审计日志，备份到文件服务器。关于文件服务器配置，参考如何配置文件服务器? 。

14.7 如何清理审计日志?

超级管理员可以在系统设置 > 系统 > 定期任务 > 审计数据清理中配置审计日志的定期清理。

14.12 登录时如提示磁盘空间占用大于80%或不足5GB的告警如何处理?

对运维审计系统的磁盘空间占用最多的是审计日志，因此当磁盘空间占用超过80%时，可以将审计日志导出备份，并在运维审计系统上清理审计日志，具体方法如下：

1. **使用超级管理员帐号登录运维审计系统。**
2. **选择系统设置 > 系统 > 定期任务 > 审计数据备份。**
3. **在手动备份界面，设置文件服务器信息后单击确定，将审计数据备份到文件服务器中。**

   Attention: 请确保将被清理的所有数据，都已在文件服务器上进行了备份。
4. **选择系统设置 > 系统 > 定期任务 > 审计数据清理。**
5. **选择启用，开启审计数据清理。**
6. **设置定期清理时间和天数，单击确定。**

   设置审计数据清理任务后，运维审计系统将在每天指定的时间清理设置天数之前的审计数据，从而实现释放磁盘空间并清除告警的目的。