文档ID118012

已更新：2015年5月20日

贡献用Nazmul Rajib， Cisco TAC工程师。

下载 pdf文档
打印
[+] 反馈

相关产品

- 思科FireSIGHT管理中心750
- 思科FireSIGHT管理中心3500
- 思科FireSIGHT管理中心1500
- 思科FireSIGHT管理中心
- 思科FireSIGHT管理中心虚拟设备

目录

简介
先决条件
要求
使用的组件
故障排除
步骤 1：确定存储的事件数量
步骤 2： 确定日志选项
步骤 3： 调节连接数据库的大小
相关信息
相关的思科支持社区讨论

简介

本文描述如何确定根本原因和排除故障问题，当连接事件从FireSIGHT管理中心时消失，在系统几天后运行。它也许发生由于管理中心的配置设置。

先决条件

要求

思科建议您有FireSIGHT管理中心知识。

使用的组件

本文档中的信息基于下列硬件和软件版本：

- FireSIGHT管理中心
- 软件版本5.2或以上

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

故障排除

步骤 1：确定存储的事件数量

为了确定在FireSIGHT管理中心存储连接事件的数量，

1. 选择**分析>连接>连接事件表查阅**。
2. 展开时间窗对包含所有时事的大范围，例如12个月。
3. 注释行总数在页底端。点击最后一页并且注释最后可用的连接事件的时间戳。

此信息给予您想法多少，并且您多久能保留与您的当前配置的连接事件。

步骤 2：

查看哪些连接被记录，并且在流的地方连接被记录。您应该记录连接符合您的组织安全和标准需要。如果您的目标是限制您生成事件的数量，规则的仅启用日志关键对您的分析。然而，如果想要您的网络流量一个大局，您能启用日志另外的访问控制规则的或默认操作的。您能禁用非本质流量的连接记录日志为了帮助保留长时间的连接事件。

> **提示**：为了优化性能，思科建议您记录开始处或连接的结束，但是不是两个。

> **注意**：对于单个连接， END连接事件包含在会话的持续时间期间收集的所有在开始处连接事件的信息以及信息。对于托拉斯和请允许规则，它推荐使用END连接。

此图表解释不同的日志选项可用为每规则操作：

规则操作或日志选项	日志在开始	在末端的日志
托拉斯 默认操作:托拉斯	X	X
准许 默认操作:入侵	X	X
默认操作:发现号 箴言报		x (必需)
块 有重置的块	X	

Defaut操作：块 交互块 有重置的交互块 安全智能	 X X	 x (如果绕过)

步骤 3：

连接事件取决被修剪的于最大连接事件设置于系统策略。为了更改设置：

1. 选择**系统>本地>System策略**。
2. 点击*铅笔*图标为了编辑当前应用的策略。
3. 选择**数据库>连接数据库>Maximum连接事件**。
4. 更改**最大连接事件的**值。
5. 点击**保存策略和退出**，然后**适用于**策略您的设备。

可以存储的最大数量连接事件取决于管理中心型号：

> **注意**：最大事件限制共享在连接事件和安全智能事件之间;配置的最大值的总和两个事件的不可以超过最大事件限制。

管理中心型号	**事件最大**
FS750，DC750	50百万
FS1500，DC1500	100百万
FS2000	300百万
FS3500，DC3500	500百万
FS4000	10亿
虚拟设备	10百万

> **警告**：在数据库限额的一增加能有在设备的相反性能影响。为了改进性能，您应该为事件限额专门制作您有规律地工作与事件的数量。

对于显示在时间范围的事件计数的小部件，事件的总数也许不反射详细数据是可用的在事件查看器事件的数量。因为系统有时修剪更旧的事件详细信息管理磁盘空间使用情况，这发生。为了最小化修剪事件详细信息的出现，您能优化事件日志记录仅那些事件最重要对您的部署。

相关信息

- **配置数据库事件限额**
- 技术支持和文档 - Cisco Systems

相关的思科支持社区讨论

思科支持社区是提出和解答问题、分享建议以及与同行协作的论坛。

有关本文档中所用的规则信息，请参阅 Cisco Technical Tips Conventions 。

已更新：2015年5月20日
文档ID118012