连接事件似乎从FireSIGHT管理中心消失

目录

简介

本文档介绍如何确定根本原因，以及如何解决系统运行几天后连接事件从FireSIGHT管理中心消失的问题。这可能是由于管理中心的配置设置造成的。

先决条件

要求

Cisco建议您了解FireSIGHT管理中心。

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
- 5.2 或更高软件版本

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：确定存储事件的数量

要确定FireSIGHT管理中心上存储的连接事件数量，

1. 选择**Analysis > Connections > Table View of Connection Events**。
2. 将“时间窗口”扩展为包含所有当前事件的范围，例如12个月。
3. 请注意页面底部的总行数。单击最后一页并记下上次可用连接事件的时间戳。

此信息可让您了解使用当前配置可以保留连接事件的数量和持续时间。

步骤 2：确定日志记录选项

查看记录哪些连接，以及连接记录到的流中的位置。您应根据贵组织的安全和合规性需求记录连接。如果您的目标是限制生成的事件数量，则仅对分析至关重要的规则启用日志记录。但是，如果您希望获得网络流量的广泛视图，则可以启用其他访问控制规则或默认操作的日志记录。您可以禁用非基本流量的连接日志记录，以帮助将连接事件保留更长时间。

> **提示：**为了优化性能，Cisco建议您记录连接的开始或结束，而不是同时记录两者。

> **注意：**对于单个连接，连接结束事件包含连接开始事件中的所有信息以及在会话期间收集的信息。对于信任和允许规则，建议使用连接终止。

此图表说明了可用于每个规则操作的不同日志记录选项：

规则操作或日志记录选项	开始时记录	结束时记录
信任 默认操作:信任	X	X
允许 默认操作:入侵	X	X
默认操作:发现 监控		X（必填）
阻止 阻止并重置	X	
默认操作：阻止 交互式块 交互式阻止并重置	X	X（如果绕过）
安全情报	X	

步骤 3：调整连接数据库的大小

根据系统策略中的Maximum Connection Events设置删除连接事件。要更改设置，请执行以下操作：

1. 选择**System > Local > System Policy**。
2. 单击*铅笔*图标以编辑当前应用的策略。
3. 选择**Database > Connection Database > Maximum Connection Events**。
4. 更改**Maximum Connection Events**的值。
5. 单击**Save Policy and Exit**，然后单击**Apply the policy**应用到设备。

可存储的最大连接事件数量取决于管理中心型号：

注意：最大事件限制在连接事件和安全情报事件之间共享；两个事件的配置最大值之和不能超过最大事件限制。

管理中心模型	最大事件数
FS750、DC750	5000万
FS1500、DC1500	1亿
FS2000	3亿
FS3500、DC3500	5亿
FS4000	10亿
虚拟设备	1000万

警告：数据库限制增加可能会对设备性能造成负面影响。为了提高性能，您应该定制事件限制来限制定期处理的事件数量。

对于在时间范围内显示事件计数的构件，事件总数可能无法反映事件查看器中可用的详细数据事件数。出现这种情况是因为系统有时会删除较旧的事件详细信息以管理磁盘空间使用情况。为了最大限度地减少事件详细信息修剪的发生，您可以微调事件日志记录，以仅记录对部署最重要的事件。

相关信息

- 配置数据库事件限制
- 技术支持和文档 - Cisco Systems

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。