目录

简介

如果登录使用远程桌面协议(RDP)的远程主机，并且远程用户名跟您的用户不同， FireSIGHT系统更改关联与您的在FireSIGHT管理中心的IP地址用户的IP地址。它关于访问控制规则引起在权限上的变化用户的。您注意不正确用户关联与工作站。本文为此问题提供解决方案。

先决条件

思科建议您有在FireSIGHT系统和用户代理的知识。

> **注意**：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。

根本原因

此问题发生由于对Windows安全的认证尝试注册域控制器的方式Microsoft活动Directory(AD)日志RDP。AD记录RDP会话的认证尝试源主机IP地址而不是您连接的RDP终端。如果登录有不同的用户帐户的远程主机，这将更改用户关联与您的原始工作站IP地址。

验证

要验证此是什么发生，您能验证从登录事件的IP地址从您的原始工作站和RDP远程主机有同样IP地址。

要查找这些事件，您将需要遵从下面的步骤：

步骤 1：确定您主机验证的域控制器：

运行以下命令：

示例输出：

开始“DC:的线路”将是开始“地址域控制器和线路的名称：” IP地址。

步骤 2：使用RDP请登录在Step1识别的域控制器

步骤 3：去**Start > Administrative Tools > Event Viewer**。

步骤 4：下来查询对**Windows日志> Security**。

步骤 5：您的工作站的IP地址的过滤器通过单击过滤器当前日志，单击XML选项卡和单击编辑查询。

步骤 6：参与以下XML查询，替代您的IP地址用< IP地址>

步骤 7：点击**登录事件**并且点击**详细信息选项卡**。

一个输出示例：

在登陆以后完成这些同样步骤通过RDP，并且您注意您将接收另一个登录事件(事件ID 4624)用IP地址和显示一样由从登录事件XML数据的以下线路从原始登录：

解决方案

要缓和此问题，如果使用用户代理2.1以上，您能排除您的所有帐户
使用主要RDP在用户代理配置里。

步骤 1：登录用户代理主机。

步骤 2：启动用户代理用户界面。

步骤 3：点击**不包括用户名**选项卡。

步骤 4：输入您希望排除的所有用户名。

步骤 5：单击 **Save**。

在此列表输入的用户不生成在FireSIGHT管理中心的登录事件并且不将是
关联对IP地址。