# 从Windows 7/Vista客户端的流量显示工作站而不是访问日志的用户

## 目录



## 问题

从Windows 7/Vista客户端的流量为什么显示工作站而不是访问日志的用户？

## 环境

Microsoft Windows 7， Microsoft Windows Vista，思科Web安全工具(所有版本)，代理人类型：IP地址

## 症状

在访问日志的某些记录行显示计算机机器名字，而不是域\用户。

Microsoft介绍新特性到Windows 7，并且Windows比斯塔呼叫“网络连通性状态指示” (NCSI)，出现作为一个小的地球图标在系统托盘的网络接口图标出现。在登录之后，此功能将尝试请求从互联网的数据为了知道是否有Internet连接。

有与NCSI的已知问题，将发送计算机凭证而不是用户凭证，当NTLM验证要求时。

因为NCSI是很可能发送从PC的第一请求到WSA，没有请指定代理存在，和有机器名字的一个新的基于IP的代理人而不是实际用户名创建。此代理人使用从初始IP地址的每请求直到代理人时代，并且用户必须重新鉴别，与实时凭证的这次。

因为机器名字很可能不是最初打算的AD组的成员所有请求不会触发正确访问/解密策略，有时造成阻塞的请求。

关于NCSI的更多信息，请参阅以下Microsoft KB条款。

请参阅如下说明对应急方案问题：

1. 通过搜索启动登记编辑“regedit”从任务菜单。您必须用鼠标右键单击和选择"Run as

Administrator"。

2. 导航对：HKEY_LOCAL_MACHINE \系统\ Currentcontrolset \服务\ NlaSvc \参数\互联网

3. 在互联网密钥，双击“EnableActiveProbing”下，然后在值数据，请键入：0。
4. 点击"OK"。

5. 重新启动计算机。

这些更改可以推送对所有客户端作为一个全局策略对象(GPO)使用域控制器。

# 在WSA的应急方案

创建NCSI的一标识并且从根据URL或其用户代理的验证豁免它。

### NCSI连接的已知URL

ncsi.glbdns.microsoft.com
newncsi.glbdns.microsoft.com
www.msftncsi.com

### NCSI用户代理

Microsoft NCSI