

# 來自Windows 7/Vista客戶端的流量在訪問日誌中顯示工作站而不是使用者

## 目錄

[問題](#)

[環境](#)

[症狀](#)

[WSA的解決方法](#)

## 問題

為什麼Windows 7/Vista客戶端的流量在訪問日誌中顯示的是工作站而不是使用者？

## 環境

Microsoft Windows 7、Microsoft Windows Vista、思科網路安全裝置（所有版本）、代理型別：IP位址

## 症狀

訪問日誌中的某些日誌行顯示的是電腦名稱，而不是DOMAIN\USER。

Microsoft在Windows 7和Windows Vista中引入了一項名為「網路連線狀態指示器」(NCSI)的新功能，該功能以一個小小的全域性圖示顯示，顯示在系統托盤中的網路介面圖示上。登入後，此功能將立即嘗試從Internet請求資料，以便瞭解是否存在Internet連線。

NCSI存在已知問題，在需要NTLM身份驗證時，它將傳送電腦憑據而不是使用者憑據。

因為NCSI最有可能將來自PC的第一個請求傳送到WSA，所以還不存在替代，並且會建立一個新的基於IP的替代，該替代使用電腦名而不是實際使用者名稱。此替代項用於來自初始IP地址的每個請求，直到替代項超時，並且使用者必須重新進行身份驗證（這次使用真實憑據）。

由於電腦名稱很可能不是最初預定的AD組的成員，因此所有請求都不會觸發正確的訪問/解密策略，有時會導致請求被阻止。

有關NCSI的詳細資訊，請參閱以下[Microsoft知識庫文章](#)。

請參閱以下說明以解決此問題：

1. 從任務選單中搜尋「regedit」，啟動登錄檔編輯器。必須按一下右鍵並選擇「以管理員身份運

行」。

## 2. 導覽至

: HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\NlaSvc\Parameters\Internet

3. 在Internet金鑰下，按兩下「EnableActiveProbing」，然後在Value data中鍵入：0.

4. 按一下「確定」。

5. 重新啟動電腦。

可以使用域控制器將這些更改作為全域性策略對象(GPO)推送到所有客戶端。

## WSA的解決方法

為NCSI建立身份，使其免於基於URL或其使用者代理進行身份驗證。

### NCSI連線的已知URL

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

### NCSI使用者代理

Microsoft NCSI