

# 帶有身份驗證和多個WSA的WCCP會導致環路 ( 限制客戶端訪問需要ACL )

## 目錄

[問題](#)

[症狀](#)

[解決方案](#)

## 問題

帶有身份驗證和多個WSA的WCCP是否會造成環路 ( 限制客戶端訪問需要ACL ) ？

## 症狀

使用WCCP、身份驗證和至少兩個WSA時，客戶端在嘗試訪問透明身份驗證伺服器URL時將被重定向。這在客戶端上顯示為嚴重延遲或超時。

## 解決方案

當WCCP使用身份驗證時，WSA必須先將客戶端重定向到其自身，然後才能執行身份驗證。這是必要步驟，因為不能對同一目標執行兩次身份驗證。

發生的問題是當客戶端對WSA發出新請求時，WCCP路由器正在通過WCCP池重新定向該請求。此請求可以通過不同的WSA重新代理，這將導致第二個WSA嘗試從第一個WSA獲取對象。

為了防止這種不期望的行為，需要在WCCP路由器上建立ACL。ACL應類似於以下內容：

ACL行	目的
access-list 105 deny ip host <WSA 1> any	請勿重定向來自WSA 1的流量
access-list 105 deny ip host <WSA 2> any	請勿重定向來自WSA 2的流量
access-list 105 deny ip host any <WSA 2>	請勿將任何客戶端重定向到WSA 1 ( 身份驗證 )
access-list 105 deny ip host any <WSA 1>	請勿將任何客戶端重定向到WSA 2 ( 身份驗證 )

這將防止將客戶端重定向到WSA的代理身份驗證請求。

您還可以利用組清單來限制接受哪些WSA作為Web快取：

ACL行	目的
access-list 15 permit <WSA 1>	允許將此IP包括在指定的WCCP服務ID中
access-list 15 permit <WSA 2>	允許將此IP包括在指定的WCCP服務ID中

使用這些ACL實作WCCP的語法為：

```
ip wccp <service ID> redirect-list 105
```

```
ip wccp <service ID> redirect-list 105 group-list 15
```

**附註：**您需要為擁有的每個WSA新增規則。在上述場景中，只有兩個WSA。