為什麼在訪問日誌中記錄電腦名稱或NULL使用者名稱？

目錄

問題

- 為什麼在訪問日誌中記錄電腦名稱或NULL使用者名稱？
- 您如何識別使用工作站或NULL憑證進行後續身份驗證豁免的請求？

環境

- 思科網路安全裝置(WSA) — 所有版本
- 具有IP代理的身份驗證方案NTLMSSP
- Windows Vista及更新的案頭和移動Microsoft作業系統

症狀

WSA阻止來自某些使用者的請求或行為異常。
訪問日誌顯示電腦名稱或NULL使用者名稱和域，而不是使用者ID。

此問題會在以下時間後自行解決：

- 代理超時（代理超時預設值為60分鐘）
- 重新啟動代理進程(CLI命令> *diagnostic* > *proxy* > *kick*)
- 刷新身份驗證快取(CLI命令> *authcache* > *flushall*)

背景資訊

在Microsoft作業系統的最新版本中，應用程式不再要求實際使用者登入才能向Internet傳送請求。當WSA收到這些請求並請求進行身份驗證時，客戶端工作站沒有可用於身份驗證的使用者憑據，而客戶端工作站可能會使用電腦的電腦名稱作為替代項。

WSA將獲取提供的電腦名稱，並將其轉發到Active Directory(AD)，由其進行驗證。

通過有效的身份驗證，WSA建立一個IP代理，將電腦的工作站名稱繫結到工作站的IP地址。來自同

一IP的其他請求將使用代理，因而使用工作站名稱。

如果工作站名稱不是任何AD組的成員，則請求可能不會觸發預期的訪問策略，因而被阻止。問題一直存在，直到替代超時，並且必須更新身份驗證。這一次，在實際使用者登入且有效的使用者憑據可用時，將使用此資訊建立新的IP代理，並且進一步的請求將與預期的訪問策略匹配。

另一個出現的情況是應用程式傳送無效憑據（NULL使用者名稱和NULL域）和無效電腦憑據。這被視為身份驗證失敗，將被阻止；或者，如果啟用了訪客策略，則失敗的身份驗證將被視為「訪客」。

工作站名稱以**$**後跟**@DOMAIN**結尾，這樣便可通過在**$@**的accesslogs上使用CLI命令**grep**來跟蹤工作站名稱。有關說明，請參閱以下示例。

```
> grep $@ accesslogs

1332164800.0000 9 10.20.30.40 TCP_DENIED/403 5608 GET http://www.someURL.com
"gb0000d01$@DOMAIN" NONE/- - BLOCK_WEBCAT_11-DefaultGroup-Internet-NONE-NONE-
NONE-NONE <-,-,"-","-",-,-,-,"-","-",-,-,"-",-,"-","-",-,"-","-","-","-","-","-",
0.00,0,-,"-","-"> -
```

上面一行顯示已為IP地址10.20.30.40和電腦名稱**gb0000d01$建立IP代理的示**

為了查詢傳送電腦名的請求，必須確定特定IP地址的工作站名稱首次出現的位置。以下CLI命令可完成以下操作：

```
> grep 10.20.30.40 -p accesslogs
```

搜尋第一次出現的工作站名稱的結果。三個第一次請求通常被識別為NTLM單一登入(NTLMSSP/NTLMSSP)握手，如下面的示例所示:

```
1335248044.836 0 10.20.30.40 TCP_DENIED/407 1733 GET http://SomeOtherURL.com -
NONE/- - OTHER-NONE-DefaultGroup-NONE-NONE-NONE-NONE
<-,-,"-","-",-,-,-,"-","-",-,-,"-",-,"-","-",-,"-","-","-","-","-","-",
0.00,0,-,"-","-"> -

1335248044.839 0 10.20.30.40 TCP_DENIED/407 483 GET http://SomeOtherURL.com -
NONE/- - OTHER-NONE-DefaultGroup-NONE-NONE-NONE-NONE
<-,-,"-","-",-,-,-,"-","-",-,-,"-",-,"-","-",-,"-","-","-","-","-","-",
0.00,0,-,"-","-"> -

1335248044.845 10 10.20.30.40 TCP_DENIED/403 2357 GET http://SomeOtherURL.com
"gb0000d01$@DOMAIN" NONE/- - BLOCK_ADMIN_PROTOCOL_11-DefaultGroup-DefaultGroup-
DefaultGroup-NONE-NONE-NONE
<-,-,"-","-",-,-,-,"-","-",-,-,"-",-,"-","-",-,"-","-","-","-","-","-",
0.00,0,-,"-","-"> -
```

進行故障排除時，請確保這些請求針對同一個URL，並以非常短的時間間隔記錄，表明它是自動NTLMSSP握手。

在上方示例中，對於顯式請求，使用HTTP響應代碼407（需要代理身份驗證）記錄前面的請求，而使用HTTP響應代碼401（未經身份驗證）記錄透明請求。

AsyncOS 7.5.0及更高版本上提供了一項新功能，您可以在其中為電腦憑據定義不同的代理超時。可以使用以下命令進行配置：

```
> advancedproxyconfigChoose a parameter group:- AUTHENTICATION - Authentication
related parameters- CACHING - Proxy Caching related parameters- DNS - DNS related
parameters- EUN - EUN related parameters- NATIVEFTP - Native FTP related parameters-
FTPOVERHTTP - FTP Over HTTP related parameters- HTTPS - HTTPS related parameters-
SCANNING - Scanning related parameters- WCCP - WCCPv2 related parameters-
MISCELLANEOUS - Miscellaneous proxy relatedparameters[]> AUTHENTICATION...Enter the
surrogate timeout.[3600]>Enter the surrogate timeout for machine credentials.[10]>.
```

可以使用相同的步驟檢測哪些請求獲得了傳送的NULL憑據，並發現哪個URL或使用者代理正在傳送無效憑據並免除對其進行身份驗證。

免除URL身份驗證

為了防止此請求導致建立虛假代理，必須免除URL的身份驗證。或者，您可能決定免除了傳送請求本身的身份驗證，而是確保使任何請求免除身份驗證，而不是免除URL的身份驗證。可以通過在WSA的accesslog訂閱的可選**Custom Fields**中新增附加引數**%u**來新增要記錄到訪問日誌中的使用者代理。識別使用者代理後，必須免除其身份驗證。