AnyConnect 4.0版和NAC狀態代理在ISE故障排除指南上未彈出

目錄

簡介

身分識別服務引擎(ISE)提供定位功能，要求使用網路准入控制(NAC)代理（適用於Microsoft Windows、Macintosh或通過Web代理）或AnyConnect版本4.0。AnyConnect版本4.0 ISE狀態模組的工作方式與NAC代理完全相同，因此在本文檔中稱為NAC代理。客戶端狀態故障的最常見症狀是NAC代理沒有彈出，因為工作情況始終會導致NAC代理視窗彈出並分析PC。本文檔可幫助您縮小導致終端安全評估失敗的眾多原因的範圍，這意味著NAC代理不會彈出。這不是為了詳盡無遺，因為NAC代理日誌只能由思科技術協助中心(TAC)進行解碼，且可能的原因眾多；然而，它旨在澄清情況並更準確地查明問題，而不是簡單地「代理不會彈出狀態分析」，並且可能有助於您解決最常見的原因。

必要條件

需求

初始設定完成後，會編寫本文檔中列出的場景、症狀和步驟供您排除故障。有關初始配置，請參閱Cisco.com上的Cisco ISE配置指南上的終端安全評估服務。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- ISE版本1.2.x
- 適用於ISE的NAC代理4.9.x版
- AnyConnect版本4.0

附註：該資訊也應適用於ISE的其他版本，除非版本說明指明主要行為更改。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

故障排除方法

是什麼讓特工彈出來？

代理在發現ISE節點時彈出。如果代理檢測到它沒有完全網路訪問並且處於狀態重定向情況，則它會持續查詢ISE節點。

有一個Cisco.com文檔說明了代理發現過程的詳細資訊：適用於身分識別服務引擎的網路認可控制(NAC)代理探索程式。為了避免內容重複，本文檔僅討論要點。

客戶端連線時，會進行RADIUS驗證（MAC過濾或802.1x），最後ISE將重新導向存取控制清單(ACL)和重新導向URL返回網路裝置(交換器、調適型安全裝置(ASA)或無線控制器)，以限制客戶端流量僅允許其取得IP位址和網域名稱伺服器(DNS)解析。來自客戶端的所有HTTP(S)流量都會重定向到ISE上以CPP（客戶端狀態和調配）結尾的唯一URL，但目的地為ISE門戶本身的流量除外。NAC代理將常規HTTP GET資料包傳送到預設網關。如果代理沒有收到任何答案或除CPP重定向之外的任何其他答案，則代理認為自己具有完全連線，並且不進行情況分析。如果它收到的HTTP響應是重定向到特定ISE節點末尾的CPP URL，則它繼續狀態進程並聯絡該ISE節點。它僅在成功從該ISE節點接收終端安全評估詳細資訊時彈出並開始分析。

NAC代理還連線到配置的發現主機IP地址（它預計不會配置多個地址）。 也期望重新導向，以便取得具有作業階段ID的重新導向URL。如果發現IP地址是ISE節點，則它不會繼續執行，因為它等待重定向以獲取正確的會話ID。因此，通常不需要發現主機，但將其設定為重定向ACL範圍內的任何IP地址時（例如，在VPN方案中）會非常有用。

可能的原因

不會發生重新導向

這是迄今為止最常見的原因。若要驗證或無效，請在代理未彈出的PC上開啟瀏覽器，並在鍵入任何URL時檢視是否重定向到狀態代理下載頁面。您也可以輸入隨機IP位址(例如http://1.2.3.4)，以避免可能出現的DNS問題（如果IP位址重新導向，但網站名稱沒有重新導向，您可以檢視DNS）。

如果您被重定向，您應該收集代理日誌和ISE支援捆綁包（使用狀態和swiss模組以調試模式）並聯絡思科TAC。這表示代理發現ISE節點，但在獲取狀態資料的過程中發生故障。

如果沒有發生重新導向，則您有第一個原因，這仍需要進一步調查根本原因。一個良好的開端是檢查網路存取裝置(無線LAN控制器(WLC)或交換器)上的組態，並移至本檔案中的下一個專案。

屬性未安裝在網路裝置上

此問題是未發生重新**導向方案的子**案例。如果未發生重新導向，第一件事是驗證（由於問題發生在

給定客戶端上），交換機或無線接入層是否正確將客戶端置於正確的狀態。

以下是在使用者端連線的交換器上執行**show access-session interface <interface number> detail** 指令(在某些平台上，您也許必須在結尾新增**detail**)的範例輸出。您必須驗證狀態是否為「Authz success」，URL重定向ACL是否正確指向預期的重定向ACL，以及URL重定向是否指向URL末尾帶有**CPP**的預期ISE節點。ACS ACL欄位不是必填欄位，因為它只顯示您在ISE上的授權配置檔案中是否配置了可下載的訪問清單。但是，必須檢查它並驗證與重定向ACL之間沒有衝突（如果存在疑問，請參閱有關狀態配置的文檔）。

```
01-SW3750-access#show access-sess gi1/0/12 det
Interface: GigabitEthernet1/0/12
MAC Address:  000f.b049.5c4b
          IP Address:  192.168.33.201
           User-Name:  00-0F-B0-49-5C-4B
              Status:  Authz Success
              Domain:  DATA
     Security Policy:  Should Secure
     Security Status:  Unsecure
      Oper host mode:  single-host
    Oper control dir:  both
       Authorized By:  Authentication Server
         Vlan Policy:  N/A
             ACS ACL:  xACSACLx-IP-myDACL-51519b43
    URL Redirect ACL:  redirect
        URL Redirect:  https://ISE2.wlaaan.com:8443/guestportal/gateway?
sessionId=C0A82102000002D8489E0E84&action=cpp
     Session timeout:  N/A
        Idle timeout:  N/A
   Common Session ID:  C0A82102000002D8489E0E84
     Acct Session ID:  0x000002FA
              Handle:  0xF60002D9

Runnable methods list:

      Method   State
      mab      Authc Success
```

若要對執行AireOS的WLC進行疑難排解，請輸入**show wireless client detail <mac address>**，然後輸入**show wireless client mac-address <mac address> detail**，對執行Cisco IOS-XE的WLC進行疑難排解。系統會顯示類似的資料，您必須驗證重新導向URL和ACL，以及使用者端是否處於「POSTURE_REQD」狀態或類似情況（視軟體版本而定）。

如果屬性不存在，您必須在您正在疑難排解的客戶端的ISE中開啟身份驗證詳細資訊(導航到**Operations > Authentications**)，並在Result部分驗證重定向屬性已傳送。如果未傳送這些屬性，您應檢視授權策略，以便瞭解為什麼沒有為此特定客戶端返回屬性。可能有一個條件不匹配，因此最好逐個進行故障排除。

請記得，在重新導向ACL方面，Cisco IOS®重新導向於permit陳述式（因此ISE和DNS IP位址需要拒絕），而WLC上的AireOS重新導向於deny陳述式（因此允許用於ISE和DNS）。

屬性已就緒，但網路裝置沒有重定向

此案例的主要原因是配置問題。您應根據Cisco.com上的配置指南和配置示例檢視網路裝置的配置。如果是這種情況，問題通常存在於網路裝置的所有埠或接入點(AP)中。如果不是，則問題可能只出現在某些交換機埠或某些AP上。如果是這種情況，您應該將發生問題的埠的配置與狀態正常運行的埠或AP的配置進行比較。

FlexConnect AP是敏感的，因為它們都可以具有唯一的配置，而且在一些AP中的ACL或VLAN中很容易出錯，而其他的AP則不然。

另一個常見問題是客戶端VLAN沒有SVI。這僅適用於交換機，在Catalyst 3750系列交換機上的ISE流量重定向中會詳細討論。從屬性的角度來看，一切可能看起來都很好。

干擾可下載存取清單(DACL)

如果在重新導向屬性的同時，將DACL推回交換器（或無線控制器的Airespace-ACL），則可能會阻止您的重新導向。首先應用DACL，然後確定完全丟棄的內容以及要處理的內容。然後應用重定向ACL並確定重定向的內容。

具體來說，在大多數情況下，您需要允許您的DACL中的所有HTTP和HTTPS流量。如果封鎖此封包，系統不會將其重新導向，因為在此封包之前會將其捨棄。這不是一個安全問題，因為流量之後將主要在重新導向ACL上重新導向，因此網路上實際上不允許該流量；但是，您需要在DACL中允許這兩種型別的流量，以便它們有機會在之後立即命中重定向ACL。

NAC代理版本錯誤

很容易忘記特定NAC代理版本會針對特定ISE版本進行驗證。許多管理員升級其ISE集群，並忘記上傳客戶端調配結果資料庫中的相關NAC代理版本。

如果您的ISE代碼使用過時的NAC代理版本，請注意它可能有效，但也可能無效。因此，難怪有些客戶在工作，有些客戶卻不工作。驗證的一種方法是轉到ISE版本的Cisco.com下載部分並檢查其中存在哪些NAC代理版本。通常，每個ISE版本支援多個版本。此網頁收集所有矩陣：Cisco ISE相容性資訊。

客戶端正在使用HTTP Web代理

HTTP Web Proxy的概念是使用者端不會自行解析網站DNS IP位址，也不會直接與網站聯絡；相反，它們只需將請求傳送到代理伺服器，由代理伺服器進行處理。通常配置的典型問題是客戶端通過將網站的HTTP GET直接傳送到Proxy來解決網站(如www.cisco.com),Proxy被攔截並正確重定向到ISE門戶。但是，客戶端繼續向Proxy傳送請求，而不是隨後向ISE門戶IP地址傳送下一個HTTP GET。

如果您決定不將目的地為Proxy的HTTP流量重新導向，則您的使用者可以在不進行驗證或偽裝的情況下直接存取整個Internet（因為所有流量都會通過Proxy）。解決方案是實際修改客戶端的瀏覽器設定，並在代理設定中為ISE IP地址新增例外。這樣，當客戶端必須到達ISE時，它將請求直接傳送到ISE，而不是傳送到Proxy。這可避免無限循環，即客戶端會不斷重新導向，但永遠不會看到登入頁面。

請注意，NAC代理不受系統中輸入的代理設定的影響，它繼續正常運行。這表示如果您使用Web代理，則不能同時使NAC代理發現工作（因為它使用埠80）並在使用者瀏覽時重定向到狀態頁面後讓使用者自行安裝代理（因為使用代理埠和典型交換機無法在多個埠上重定向）。

在NAC代理中配置發現主機

特別是ISE版本1.2之後，建議不要在NAC代理上配置任何發現主機，除非您擁有有關其操作和不操作的專業知識。NAC代理應該發現通過HTTP發現對客戶端裝置進行身份驗證的ISE節點。如果您依賴發現主機，則可能讓NAC代理聯絡另一個ISE節點，而不是驗證裝置且無法正常工作的ISE節點。ISE版本1.2拒絕通過發現主機進程發現節點的代理，因為它希望NAC代理從重定向URL獲取會話

ID，因此不鼓勵使用此方法。

在某些情況下，可能需要配置發現主機。然後，應該為它配置由重定向ACL重定向的任何IP地址（即使不存在此地址），理想情況下，它不應與客戶端位於同一子網中（否則客戶端將無限期地為該地址進行ARP，並且永遠不會傳送HTTP發現資料包）。

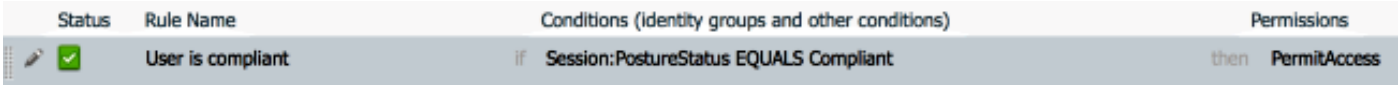
NAC代理有時不彈出

當問題更加間歇性並且拔出/更換電纜/WiFi連線等操作使其工作正常時，問題就更加微妙了。這可能是RADIUS作業階段ID的問題，其中作業階段ID是通過RADIUS記賬在ISE上刪除的（禁用記賬以檢視它是否更改了某些內容）。

如果您使用ISE版本1.2，另一種可能性是客戶端傳送許多HTTP資料包，因此沒有來自瀏覽器或NAC代理。ISE版本1.2掃描HTTP資料包中的使用者代理欄位，以檢視它是否來自NAC代理或瀏覽器，但許多其它應用程式傳送帶有使用者代理欄位的HTTP流量，並且不提及任何作業系統或有用的資訊。然後ISE版本1.2傳送授權更改以斷開客戶端。ISE版本1.3不受此問題影響，因為它以不同方式工作。解決方案是升級到版本1.3，或允許重定向ACL中所有檢測到的應用，以便它們不會重定向到ISE。

反向問題：代理重複彈出

當代理彈出、執行狀態分析、驗證客戶端，並在稍後再次彈出（而不是允許網路連線並保持靜默）時，可能會出現相反的問題。發生這種情況的原因是，即使狀態成功，HTTP流量仍重定向到ISE上的CPP門戶。接下來，最好通過ISE授權策略，檢查您是否有規則在看到合規客戶端且不再是CPP重定向時傳送允許訪問（或具有可能ACL和VLAN的類似規則）。



相關資訊

- 思科ISE配置指南上的終端安全評估服務
- 適用於ISE的NAC代理探索程式
- Catalyst 3750系列交換器上的ISE流量重新導向
- 技術支援與文件 - Cisco Systems