電腦訪問限制的優缺點

目錄

簡介

本文描述電腦訪問限制(MAR)遇到的問題，並提供該問題的解決方案。

隨著個人擁有的裝置的增長，對於系統管理員來說，越來越重要的一點是提供一種方法，限制對網路某些部分的訪問，使其僅限於企業擁有的資產。本文中描述的問題涉及如何安全地識別這些關注區域並對它們進行身份驗證，而不會中斷使用者連線。

必要條件

需求

思科建議您瞭解802.1x，以便完全瞭解本檔案。本文檔假定您熟悉使用者802.1x身份驗證，並重點介紹與使用MAR相關的問題和優勢，更一般地說，是電腦身份驗證。

採用元件

本文件所述內容不限於特定軟體和硬體版本。

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。

問題

MAR基本上嘗試解決大多數當前和流行的可擴展身份驗證協定(EAP)方法所固有的常見問題，即機器身份驗證和使用者身份驗證是相互獨立的過程。

使用者身份驗證是大多數系統管理員熟悉的802.1x身份驗證方法。其思想是為每個使用者提供憑證

（使用者名稱/密碼），該組憑證代表一個物理人員（也可以在多個使用者之間共用）。 因此，使用者可以使用這些憑證從網路中的任何位置登入。

機器身份驗證在技術上相同，但通常不會提示使用者輸入憑證（或證書）；電腦或機器自己做這件事。這要求電腦已儲存憑據。傳送的使用者名稱**為host/<MyPCHostname>**，前提是您的電腦將**<MyPCHostname>**設定為主機名。換句話說，它會傳送**主機/**後跟主機名。

雖然與Microsoft Windows和Cisco Active Directory沒有直接關係，但是如果電腦加入到Active Directory，則此過程更容易呈現，因為電腦主機名已新增到域資料庫，並且證書經過協商（預設情況下每30天更新一次）並儲存在電腦上。這意味著可以從任何型別的裝置執行電腦身份驗證，但是如果電腦已加入Active Directory且憑證對使用者保持隱藏，則進行身份驗證會更加容易和透明。

MAR即解決方案

很容易說解決方案是為思科訪問控制系統(ACS)或思科身份服務引擎(ISE)完成MAR，但在實施之前需要考慮其優缺點。如何實施這一點在ACS或ISE使用手冊中進行了最佳描述，因此本文檔簡單介紹了是否考慮該解決方案，以及一些可能的障礙。

優點

MAR的發明是因為使用者和機器身份驗證是完全分開的。因此，RADIUS伺服器無法強制進行使用者必須從公司擁有的裝置登入的驗證。使用MAR時，RADIUS伺服器（思科端的ACS或ISE）對給定的使用者身份驗證強制在X小時內（通常為8小時，但可配置）存在有效的電腦身份驗證，該身份驗證早於相同端點的使用者身份驗證。

因此，如果RADIUS伺服器知道電腦憑證，則電腦身份驗證成功，通常如果電腦已加入域，並且RADIUS伺服器通過連線到域來驗證這一點。完全由網路管理員決定，成功的電腦身份驗證是否提供網路的完全訪問許可權，還是僅提供受限訪問許可權；通常，這至少會開啟客戶端和Active Directory之間的連線，以便客戶端可以執行諸如更新使用者密碼或下載組策略對象(GPO)之類的操作。

如果使用者身份驗證來自一個裝置，而該裝置在過去幾個小時內未進行電腦身份驗證，則即使該使用者正常有效，也會拒絕該使用者。

僅當身份驗證有效且從過去幾個小時內發生電腦身份驗證的終結點完成時，才授予使用者完全訪問許可權。

缺點

本節介紹使用MAR的缺點。

MAR和Microsoft Windows請求方

MAR的理念是，要成功進行使用者身份驗證，不僅該使用者必須擁有有效憑證，而且還必須從該客戶端記錄成功的電腦身份驗證。如果有任何問題，使用者無法進行驗證。出現的問題是此功能有時可能會無意中鎖定合法客戶端，從而強制客戶端重新啟動以重新獲得對網路的訪問。

Microsoft Windows僅在啟動時（出現登入螢幕時）執行電腦身份驗證；使用者輸入使用者憑證後，即會執行使用者身份驗證。此外，如果使用者註銷（返回登入螢幕），將執行新電腦身份驗證。

以下範例情境顯示MAR有時導致問題的原因：

使用者X整天都在使用通過無線連線連線的筆記型電腦。一天結束後，他就會關掉筆記型電腦，離開工作崗位。這將使筆記型電腦進入休眠狀態。第二天，他回到辦公室，開啟筆記型電腦。現在，他無法建立無線連線。

當Microsoft Windows休眠時，它會獲取系統當前狀態的快照，其中包括登入者的上下文。使用者筆記型電腦的MAR快取條目將在夜間到期並清除。但是，當筆記型電腦通電時，它不會執行電腦身份驗證。相反，它會直接進入使用者身份驗證，因為休眠記錄的是這種情況。解決此問題的唯一方法是註銷使用者，或重新啟動電腦。

儘管MAR是一個很好的功能，但它有可能導致網路中斷。在瞭解MAR的工作原理之前，很難對這些中斷進行故障排除；在實施MAR時，必須教導終端使用者如何正確關閉電腦並在每天結束時從每台電腦註銷。

MAR和各種RADIUS伺服器

網路中有多個RADIUS伺服器通常用於負載平衡和備援。但是，並非所有RADIUS伺服器都支援共用MAR會話快取。只有ACS版本5.4及更高版本以及ISE版本2.3及更高版本支援節點之間的MAR快取同步。在這些版本之前，不可能對一個ACS/ISE伺服器執行電腦身份驗證，以及對另一個伺服器執行使用者身份驗證，因為它們彼此之間不通訊。

MAR和有線 — 無線交換

許多RADIUS伺服器的MAR快取依賴MAC位址。它只是一張表，上面有筆記型電腦的MAC地址及其上次成功進行機器身份驗證的時間戳。這樣，伺服器就可以知道客戶端在過去X小時內是否經過電腦身份驗證。

但是，如果您使用有線連線啟動筆記型電腦（從而通過有線MAC執行電腦身份驗證），然後在一天中切換到無線時，會發生什麼情況？RADIUS伺服器沒有辦法將您的無線MAC位址與您的有線MAC位址建立關聯，且無法得知您在過去的X小時內已透過電腦驗證。唯一的方法是註銷並讓Microsoft Windows通過無線方式執行其他電腦身份驗證。

解決方案

Cisco AnyConnect具有多種其他功能，其中包括預配置的配置檔案，這些配置檔案可觸發機器和使用者身份驗證。但是，會遇到與Microsoft Windows請求方相同的限制，即僅在註銷或重新啟動時進行電腦身份驗證。

此外，在AnyConnect版本3.1及更高版本中，可以通過EAP連結執行EAP-FAST。這基本上是單一身份驗證，即同時傳送兩對憑證：電腦使用者名稱/密碼和使用者使用者名稱/密碼。然後，ISE會更輕鬆地檢查兩者是否成功。由於不使用快取，也不需要檢索以前的會話，因此具有更高的可靠性。

當PC啟動時，AnyConnect僅傳送電腦身份驗證，因為沒有可用的使用者資訊。但是，在使用者登入時，AnyConnect同時傳送電腦和使用者憑證。此外，如果您斷開連線或拔下/更換電纜，電腦和使用者憑證將再次以單一EAP-FAST身份驗證傳送，這與不帶EAP連結的早期版本AnyConnect不同。

EAP-TEAP是長期最佳解決方案，因為它特別用於支援這些型別的身份驗證，但截至目前，許多OS的本地請求方仍不支援EAP-TEAP