TACACS+ 和 RADIUS 比較

目錄

簡介

用於控制網路存取的兩個主要安全通訊協定是 Cisco TACACS+ 和 RADIUS。RFC 2865 （取代 RFC 2138 ）中詳述 RADIUS 規範。 思科致力以一流的產品項目支援這兩種通訊協定。思科的用意並非與 RADIUS 競爭或影響使用者使用 TACACS+。您應選擇最能滿足自身需求的解決方案。本文件說明 TACACS+ 和 RADIUS 之間的差異，方便您做出明智的選擇。

自 1996 年二月發佈 Cisco IOS® 軟體版本 11.1 起，思科便支援 RADIUS 通訊協定。思科持續透過新特色和功能增強 RADIUS 用戶端，並作為標準支援 RADIUS。

思科開發 TACACS+ 之前，曾鄭重將 RADIUS 視為安全通訊協定進行評估。TACACS+ 通訊協定中包含許多功能，可滿足不斷成長的資安市場之需求。此通訊協定設計為可隨著網路的拓展而擴充，並隨著市場的發展適應新的資安技術。TACACS+ 通訊協定的基礎架構補充了獨立的認證、授權及計量 (AAA) 架構。

必要條件

需求

本文件沒有特定需求。

採用元件

本文件所述內容不限於特定軟體和硬體版本。

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

RADIUS 背景

RADIUS 是使用 AAA 通訊協定的存取伺服器。這是一種分散式資安系統，可保護網路和網路服務的遠端存取，防止未經授權的存取。RADIUS 由三個元件組成：

- 通訊協定，其框架格式採用使用者資料包通訊協定 (UDP)/IP。
- 伺服器。
- 用戶端。

伺服器通常在客戶據點的中央電腦上執行，而用戶端位於撥號存取伺服器中，且可分佈在整個網路中。思科已將 RADIUS 用戶端納入 Cisco IOS 軟體版本 11.1 及更新版本以及其他裝置軟體中。

用戶端/伺服器型號

網路存取伺服器 (NAS) 作為 RADIUS 的用戶端運作。用戶端負責將使用者資訊傳遞到指定的 RADIUS 伺服器，然後對傳回的回應執行動作。RADIUS 伺服器負責接收使用者連線要求、驗證使用者，並傳回用戶端向使用者提供服務所需的所有組態資訊。RADIUS 伺服器可以作為其他類型驗證伺服器的代理用戶端。

網路安全

用戶端和 RADIUS 伺服器之間的交易是透過使用共用金鑰進行驗證，而這個共用金鑰絕不會透過網路傳送。此外，在用戶端和 RADIUS 伺服器之間傳送的任何使用者密碼均經過加密處理。如此一來，便消除了在不安全網路上窺探的有心人士能確定使用者密碼的可能性。

彈性驗證機制

RADIUS 伺服器支援各種驗證使用者的方法。若隨使用者指定的使用者名和原始密碼提供，其可支援 PPP、密碼驗證通訊協定 (PAP) 或 Challenge Handshake 驗證通訊協定 (CHAP)、UNIX 登入和其他驗證機制。

伺服器程式碼可用性

有大量的伺服器程式碼發行版本可供購買和免費使用。思科伺服器包括適用於 Windows 的 Cisco Secure ACS、適用於 UNIX 的 Cisco Secure ACS 和 Cisco Access Registrar。

比較 TACACS+ 和 RADIUS

以下各節比較 TACACS+ 和 RADIUS 的多項功能。

UDP 與 TCP

RADIUS 使用 UDP，而 TACACS+ 使用 TCP。相較於 UDP，TCP 具備多項優勢。TCP 提供連線導向傳輸，而 UDP 提供盡力傳輸。RADIUS 需要額外的可程式化變數（例如重新傳輸嘗試和逾時）以補償盡力傳輸，但缺少 TCP 傳輸提供的內建支援層級：

- 無論後端驗證機制（TCP 確認）的載入和緩慢程度為何，都可透過 TCP 使用量單獨確認已在（約略）網路來回時間 (RTT) 內收到要求。
- TCP 可透過重設 (RST) 立即指出當機或未執行的伺服器。 若使用長時間執行的 TCP 連線，便可確定伺服器當機和傳回服務的時間。UDP 無法區分伺服器處於關閉狀態、伺服器速度慢伺服器不存在之間的差異。
- 使用 TCP keepalive 時，可以透過實際要求偵測頻外伺服器當機。可同時維持與多個伺服器的連線，且您只需將訊息傳送至已知啟動並執行中的伺服器即可。
- TCP 的可擴充性更高，且可適應日益增長及擁塞的網路。

封包加密

RADIUS 只會加密從用戶端傳至伺服器的存取要求封包中的密碼。封包的其餘部分並未加密。其他資訊（例如使用者名稱、授權服務和計量）可由第三方擷取。

TACACS+ 會加密封包的整個主體，但保留一個標準 TACACS+ 標頭。標頭中的欄位會指出主體是否已加密。基於偵錯目的，不加密封包主體非常有用。但是在一般操作期間，封包主體會進行完全加密，以確保通訊更安全進行。

驗證與授權

RADIUS 結合了驗證與授權功能。RADIUS 伺服器傳送到用戶端的存取接受封包中包含授權資訊，這導致難以將驗證和授權分離。

TACACS+ 使用 AAA 架構，可將 AAA 分隔開來。因此可使用獨立驗證解決方案，而這些解決方案仍然可使用 TACACS+ 進行授權和計量。例如，在 TACACS+ 中，可以使用 Kerberos 驗證和 TACACS+ 授權與計量。在 Kerberos 伺服器上進行 NAS 驗證後，系統會向 TACACS+ 伺服器要求授權資訊，而無需重新進行驗證。NAS 通知 TACACS+ 伺服器它已在 Kerberos 伺服器上成功通過驗證，然後伺服器便會提供授權資訊。

在作業階段進行期間，如果需要額外的授權檢查，存取伺服器會對 TACACS+ 伺服器進行檢查，確定使用者是否有獲得使用特定指令的權限。這麼做可更有效控制從驗證機制中分離時，可在存取伺服器上執行的指令。

多重通訊協定支援

RADIUS 不支援以下通訊協定：

- AppleTalk 遠端存取 (ARAP) 通訊協定
- NetBIOS 訊框通訊協定控制通訊協定

- NetWare 非同步服務介面 (NASI)
- X.25 PAD 連線

TACACS+ 提供多重通訊協定支援。

路由器管理

RADIUS 不允許使用者控制路由器上可執行和不可執行的指令。因此，RADIUS 在路由器管理方面不太實用，對終端服務的彈性也不高。

TACACS+ 提供兩種方法，可針對每個使用者或每個群組控制路由器指令授權。第一種方法是無論使用者是否已在指定的權限層級獲得授權，都將權限層級指派給指令，並讓路由器使用 TACACS+ 伺服器進行驗證。第二種方法是針對每個使用者或每個群組，在 TACACS+ 伺服器中明確指定允許的指令。

互通性

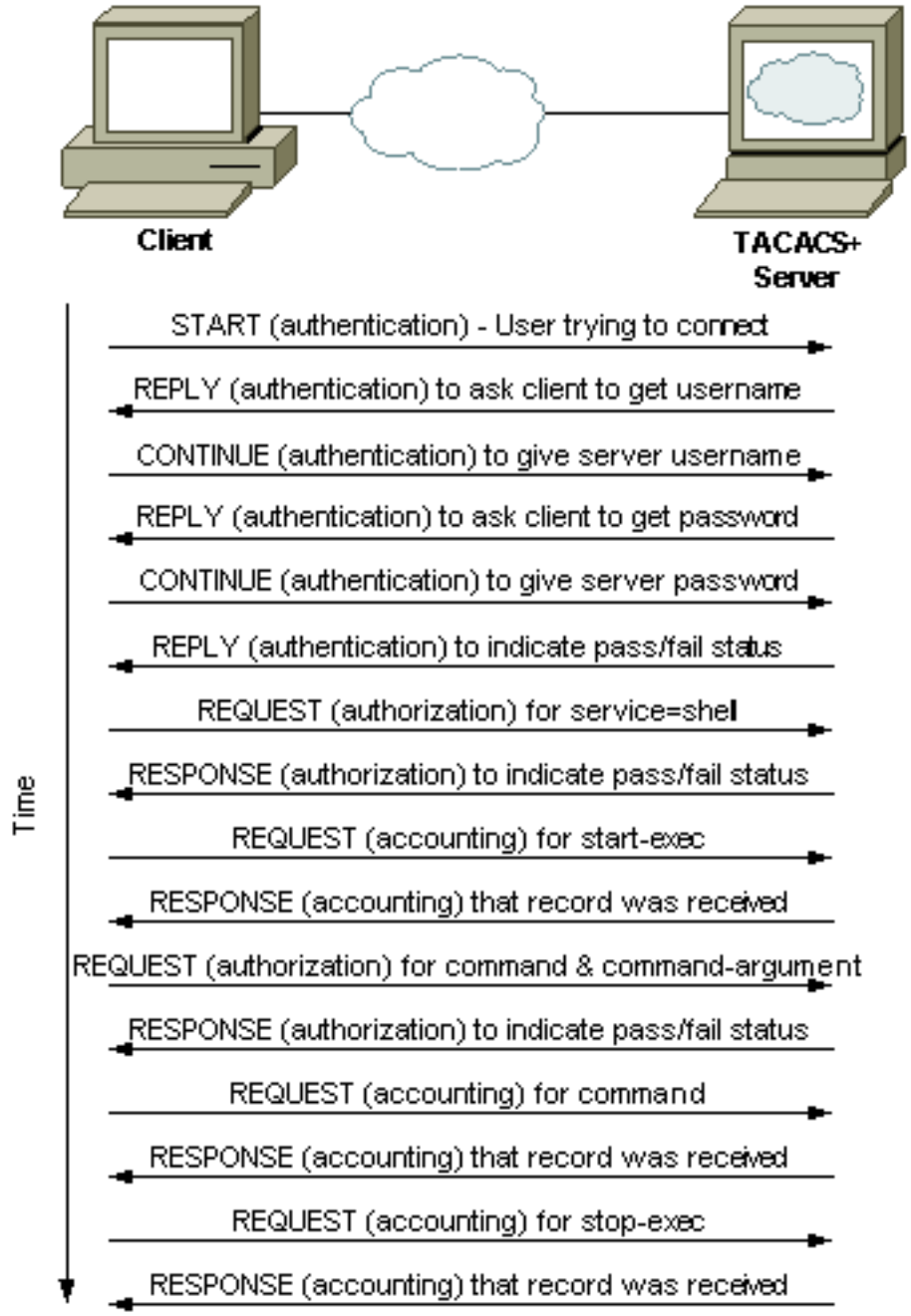
由於 RADIUS 要求建議 (RFC) 存在多種解釋，因此遵守 RADIUS RFC 並不能保證互通性。雖然有許多廠商實作 RADIUS 用戶端，但這不代表它們彼此具互通性。思科實作大部分 RADIUS 屬性，且持續增加更多。如果客戶在其伺服器中僅使用標準 RADIUS 屬性，則只要這些廠商實作相同的屬性，就可以在多個廠商之間實現互通性。然而，許多廠商實作的是專利屬性的延伸。如果客戶使用任何廠商專屬的延伸屬性，便無法實現互通性。

流量

由於先前提及的 TACACS+ 和 RADIUS 之間差異，用戶端和伺服器之間產生的流量會有所不同。以下範例說明用於透過驗證、exec 授權、指令授權（RADIUS 無法執行）、exec 計量和指令計量（RADIUS 無法執行）進行路由器管理時，用戶端與伺服器的 TACACS+ 和 RADIUS 之間的流量。

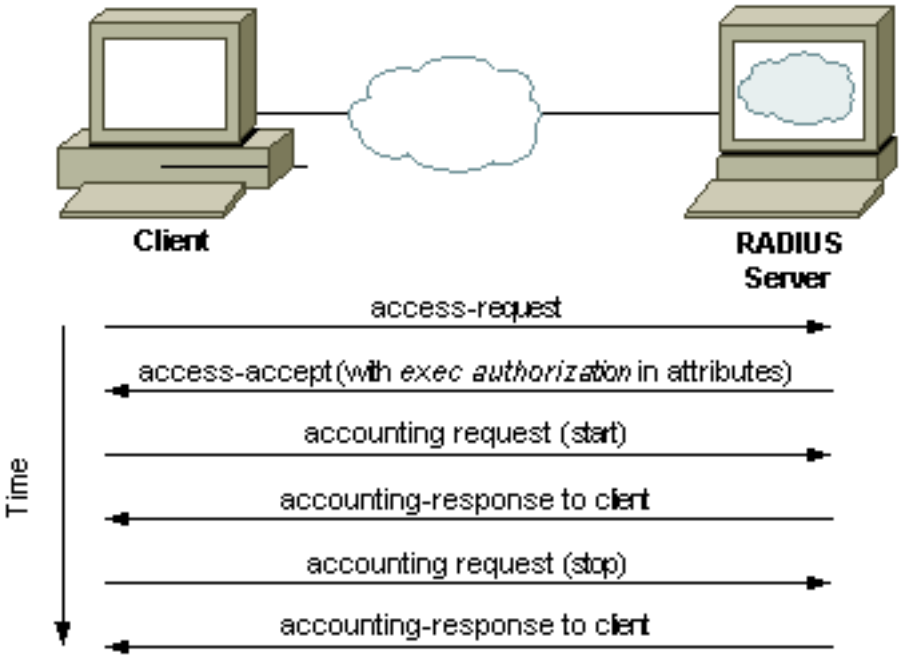
TACACS+ 流量範例

此範例假設使用者 Telnet 到路由器、執行指令並退出路由器時，透過 TACACS+ 實作登入驗證、exec 授權、指令授權、啟動停止 exec 計量和指令計量：



RADIUS 流量範例

此範例假設使用者 Telnet 到路由器、執行指令並退出路由器時（其他管理服務無法使用），透過 RADIUS 實作登入驗證、exec 授權和啟動停止 exec 計量：



裝置支援

下表列出指定平台的裝置類型對 TACACS+ 和 RADIUS AAA 的支援。其中包括新增了支援的軟體版本。如果您的產品不在此清單中，請查看產品版本資訊瞭解詳情。

思科裝置	TACACS+ 驗證	TACACS+ 授權	TACACS+ 計量	RADIUS 驗證	RADIUS 授權	RADIUS 計量
Cisco Aironet[1]	12.2(4)JA	12.2(4)JA	12.2(4)JA	所有存取點	所有存取點	所有存取點
Cisco IOS 軟體[2]	10.33	10.33	10.33[3]	11.1.1	11.1.1[4]	11.1.1[5]
Cisco Cache Engine	—	—	—	1.5	1.5[6]	—
Cisco Catalyst 交換器	2.2	5.4.1	5.4.1	5.1	5.4.1[4]	5.4.1[5]
Cisco CSS 11000 Content Services Switch	5.03	5.03	5.03	5.0	5.0[4]	—
Cisco CSS 11500 Content Services Switch	5.20	5.20	5.20	5.20	5.20[4]	—

Cisco PIX 防火牆	4.0	4.0[7]	4.2[8,5]	4.0	5.2[7]	4.2[8,5]
Cisco Catalyst 1900/2820 交換器	8.x 企業版[9]	—	—	—	—	—
Cisco Catalyst 2900XL/3500XL 交換器	11.2.(8)SA6[10]	11.2.(8)SA6[10]	11.2.(8)SA6[10]	12.0(5)WC5[1,11]	12.0(5)WC5[1,4]	12.0(5)WC5[11,5]
Cisco VPN 3000 Concentrator [6]	3.0	3.0	—	2.0[12]	2.0	2.0[12]
Cisco VPN 5000 Concentrator	—	—	—	5.2X[12]	5.2X[12]	5.2X[12]

表格附註

1. 僅終止無線用戶端，而非 Cisco IOS 軟體版本 12.2(4)JA 或更新版本以外的管理流量。在 Cisco IOS 軟體版本 12.2.(4)JA 或更新版本中，可對無線用戶端和管理流量的終止進行驗證。
2. 請查看 Feature Navigator（現已被僅供註冊客戶使用的 Software Advisor 取代）以瞭解 Cisco IOS 軟體內的平台支援。
3. Cisco IOS 軟體版本 11.1.6.3 之前的版本未實作指令計量。
4. 無指令授權。
5. 無指令計量。
6. 僅限 URL 封鎖，而非管理流量。
7. 透過 PIX 對非 VPN 流量進行授權。**註：**5.2版 — 存取清單支援，適用於存取控制清單(ACL)RADIUS廠商專用屬性(VSA)或在PIX上終止的VPN流量之TACACS+授權6.1版 — 支援在PIX上終止的VPN流量之ACL RADIUS屬性11授權6.2.2版 — 支援在PIX上終止的VPN流量之可下載ACL（具有RADIUS授權）6.2版 — 支援透過TACACS+對PIX管理流量進行授權。
8. 僅透過 PIX 對非 VPN 流量進行計量，而不對管理流量進行計量。**註：**5.2版 — 支援通過PIX對VPN客戶端TCP資料包進行記帳。
9. 僅限企業版軟體。
10. 映像需使用 8M 快閃記憶體。
11. 僅限 VPN 終止。

相關資訊

- RADIUS 支援頁面
- IOS 文件中的 TACACS+

- TACACS/TACACS+ 支援頁面
- 要求建議 (RFC)
- 技術支援與文件 - Cisco Systems