

Confronto tra TACACS+ e RADIUS

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Convenzioni](#)

[Sfondo RADIUS](#)

[Modello client/server](#)

[Sicurezza della rete](#)

[Meccanismi di autenticazione flessibili](#)

[Disponibilità del codice server](#)

[Confronta TACACS+ e RADIUS](#)

[UDP e TCP](#)

[Crittografia pacchetti](#)

[Autenticazione e autorizzazione](#)

[Supporto multiprotocollo](#)

[Gestione router](#)

[Interoperabilità](#)

[Traffico](#)

[Supporto dispositivo](#)

[Informazioni correlate](#)

Introduzione

Due importanti protocolli di sicurezza utilizzati per controllare l'accesso alle reti sono Cisco TACACS+ e RADIUS. La specifica RADIUS è descritta nella [RFC 2865](#) , che è obsoleta rispetto alla [RFC 2138](#) . Cisco si impegna a supportare entrambi i protocolli con le migliori offerte. Cisco non intende competere con RADIUS né influenzare gli utenti nell'uso di TACACS+. È consigliabile scegliere la soluzione più adatta alle proprie esigenze. In questo documento vengono illustrate le differenze tra TACACS+ e RADIUS per poter scegliere con cognizione di causa.

Cisco supporta il protocollo RADIUS dal software Cisco IOS® versione 11.1 del febbraio 1996. Cisco continua a migliorare il client RADIUS con nuove funzionalità e supporto standard di RADIUS.

Cisco ha valutato seriamente RADIUS come protocollo di sicurezza prima di sviluppare TACACS+. Il protocollo TACACS+ includeva molte funzionalità per soddisfare le esigenze del crescente mercato della sicurezza. Il protocollo è stato progettato per adattarsi alla crescita delle reti e alle nuove tecnologie di sicurezza man mano che il mercato matura. L'architettura del protocollo TACACS+ è complementare all'architettura di autenticazione, autorizzazione e accounting (AAA) indipendente.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento [Cisco sulle convenzioni nei suggerimenti tecnici](#).

Sfondo RADIUS

RADIUS è un server di accesso che utilizza il protocollo AAA. È un sistema di protezione distribuita che protegge l'accesso remoto alle reti e ai servizi di rete da accessi non autorizzati. RADIUS è costituito da tre componenti:

- Protocollo con formato di frame che utilizza il protocollo UDP (User Datagram Protocol)/IP.
- Un server.
- Un cliente.

Il server viene eseguito su un computer centrale, in genere presso la sede del cliente, mentre i client risiedono nei server di accesso remoto e possono essere distribuiti attraverso la rete. Cisco ha incorporato il client RADIUS nel software Cisco IOS versione 11.1 e successive e in altri software per dispositivi.

Modello client/server

Un server di accesso alla rete (NAS) funziona come client di RADIUS. Il client è responsabile del passaggio delle informazioni utente ai server RADIUS designati e quindi agisce sulla risposta restituita. I server RADIUS sono responsabili della ricezione delle richieste di connessione degli utenti, dell'autenticazione dell'utente e della restituzione di tutte le informazioni di configurazione necessarie al client per fornire il servizio all'utente. I server RADIUS possono fungere da client proxy per altri tipi di server di autenticazione.

Sicurezza della rete

Le transazioni tra il client e il server RADIUS vengono autenticate tramite l'utilizzo di un segreto condiviso che non viene mai inviato in rete. Inoltre, tutte le password utente vengono inviate in modo crittografato tra il client e il server RADIUS. In questo modo si evita che un utente che snooping su una rete non protetta possa determinare la password di un utente.

Meccanismi di autenticazione flessibili

Il server RADIUS supporta diversi metodi per autenticare un utente. Quando viene fornito con il

nome utente e la password originale forniti dall'utente, può supportare PPP, il protocollo PAP (Password Authentication Protocol) o il protocollo CHAP (Challenge Handshake Authentication Protocol), l'accesso UNIX e altri meccanismi di autenticazione.

Disponibilità del codice server

Sono disponibili in commercio diverse distribuzioni di codice server. I server Cisco includono Cisco Secure ACS per Windows, Cisco Secure ACS per UNIX e Cisco Access Registrar.

Confronta TACACS+ e RADIUS

In queste sezioni vengono confrontate diverse funzionalità di TACACS+ e RADIUS.

UDP e TCP

RADIUS utilizza UDP mentre TACACS+ utilizza TCP. TCP offre diversi vantaggi rispetto a UDP. Il protocollo TCP offre un trasporto orientato alla connessione, mentre il protocollo UDP garantisce la consegna nel miglior modo possibile. RADIUS richiede variabili programmabili aggiuntive, ad esempio tentativi di ritrasmissione e timeout, per compensare il trasporto con il massimo sforzo, ma non dispone del livello di supporto incorporato offerto dal trasporto TCP:

- L'utilizzo del protocollo TCP costituisce una conferma separata della ricezione di una richiesta entro un tempo di andata e ritorno (RTT, Network Round-Trip Time) (circa), indipendentemente dal livello di caricamento e di rallentamento del meccanismo di autenticazione back-end (conferma TCP).
- Il protocollo TCP fornisce l'indicazione immediata di un server arrestato in modo anomalo, o non in esecuzione, in seguito a un ripristino (RST). Se si utilizzano connessioni TCP di lunga durata, è possibile determinare quando un server si blocca e torna in servizio. UDP non è in grado di rilevare la differenza tra un server inattivo, lento e inesistente.
- Utilizzando i pacchetti keepalive TCP, gli arresti anomali del server possono essere rilevati fuori banda con le richieste effettive. Le connessioni a più server possono essere gestite contemporaneamente ed è necessario inviare messaggi solo a quelli che sono noti per essere attivi e in esecuzione.
- Il protocollo TCP è più scalabile e si adatta alle reti in crescita e congestionate.

Crittografia pacchetti

RADIUS crittografa solo la password nel pacchetto di richiesta di accesso, dal client al server. Il resto del pacchetto non è crittografato. Altre informazioni, quali il nome utente, i servizi autorizzati e la contabilità, possono essere acquisite da terze parti.

TACACS+ cripta l'intero corpo del pacchetto, ma lascia un'intestazione TACACS+ standard. All'interno dell'intestazione è presente un campo che indica se il corpo è crittografato o meno. Ai fini del debug, è utile avere il corpo dei pacchetti non crittografato. Tuttavia, durante il normale funzionamento, il corpo del pacchetto è completamente crittografato per comunicazioni più sicure.

Autenticazione e autorizzazione

RADIUS combina autenticazione e autorizzazione. I pacchetti di accettazione dell'accesso inviati

dal server RADIUS al client contengono informazioni di autorizzazione. Ciò rende difficile disaccoppiare autenticazione e autorizzazione.

TACACS+ utilizza l'architettura AAA, che separa il server AAA. Ciò consente soluzioni di autenticazione separate che possono ancora utilizzare TACACS+ per l'autorizzazione e l'accounting. Ad esempio, con TACACS+ è possibile utilizzare l'autenticazione Kerberos e l'autorizzazione e l'accounting TACACS+. Dopo aver eseguito l'autenticazione su un server Kerberos, il NAS richiede le informazioni di autorizzazione a un server TACACS+ senza dover eseguire nuovamente l'autenticazione. Il server NAS informa il server TACACS+ che è stato autenticato correttamente su un server Kerberos, quindi fornisce le informazioni di autorizzazione.

Se è necessario un ulteriore controllo delle autorizzazioni durante una sessione, il server di accesso controlla con un server TACACS+ se all'utente è stata concessa l'autorizzazione a utilizzare un particolare comando. In questo modo è possibile esercitare un maggiore controllo sui comandi che possono essere eseguiti sul server di accesso durante la separazione dal meccanismo di autenticazione.

Supporto multiprotocollo

RADIUS non supporta i protocolli seguenti:

- Protocollo ARA (AppleTalk Remote Access)
- Protocollo di controllo NetBIOS Frame Protocol
- NASI (Novell Asynchronous Services Interface)
- Connessione X.25 PAD

TACACS+ offre supporto multiprotocollo.

Gestione router

RADIUS non consente agli utenti di controllare quali comandi possono essere eseguiti su un router e quali no. Pertanto, RADIUS non è tanto utile per la gestione dei router né tanto flessibile per i servizi terminal.

TACACS+ offre due metodi per controllare l'autorizzazione dei comandi del router per utente o per gruppo. Il primo metodo consiste nell'assegnare livelli di privilegio ai comandi e fare in modo che il router verifichi con il server TACACS+ se l'utente è autorizzato o meno al livello di privilegio specificato. Il secondo metodo consiste nello specificare esplicitamente nel server TACACS+, per utente o per gruppo, i comandi consentiti.

Interoperabilità

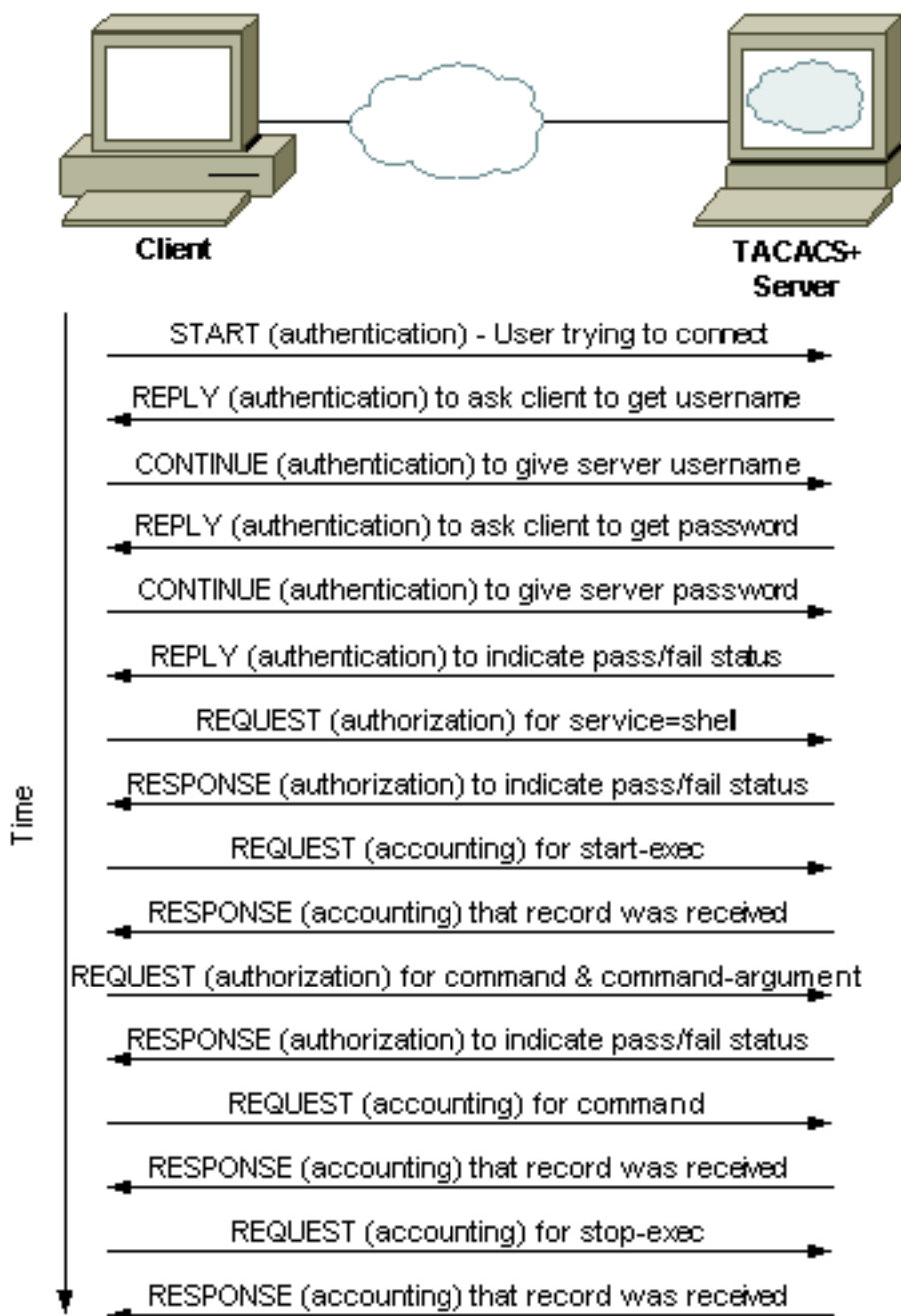
A causa di diverse interpretazioni delle RFC (Request for Comments) RADIUS, la conformità alle RFC RADIUS non garantisce l'interoperabilità. Anche se diversi fornitori implementano client RADIUS, ciò non significa che siano interoperabili. Cisco implementa la maggior parte degli attributi RADIUS e ne aggiunge costantemente altri. Se nei server vengono utilizzati solo gli attributi RADIUS standard, i clienti possono interagire tra più fornitori purché questi ultimi implementino gli stessi attributi. Tuttavia, molti fornitori implementano estensioni che sono attributi proprietari. Se un cliente utilizza uno di questi attributi estesi specifici del fornitore, l'interoperabilità non è possibile.

Traffico

A causa delle differenze sopra citate tra TACACS+ e RADIUS, la quantità di traffico generata tra il client e il server è diversa. In questi esempi viene mostrato il traffico tra il client e il server per TACACS+ e RADIUS quando usato per la gestione dei router con autenticazione, autorizzazione di esecuzione, autorizzazione dei comandi (operazione non consentita da RADIUS), accounting di esecuzione e accounting dei comandi (operazione non consentita da RADIUS).

Esempio di traffico TACACS+

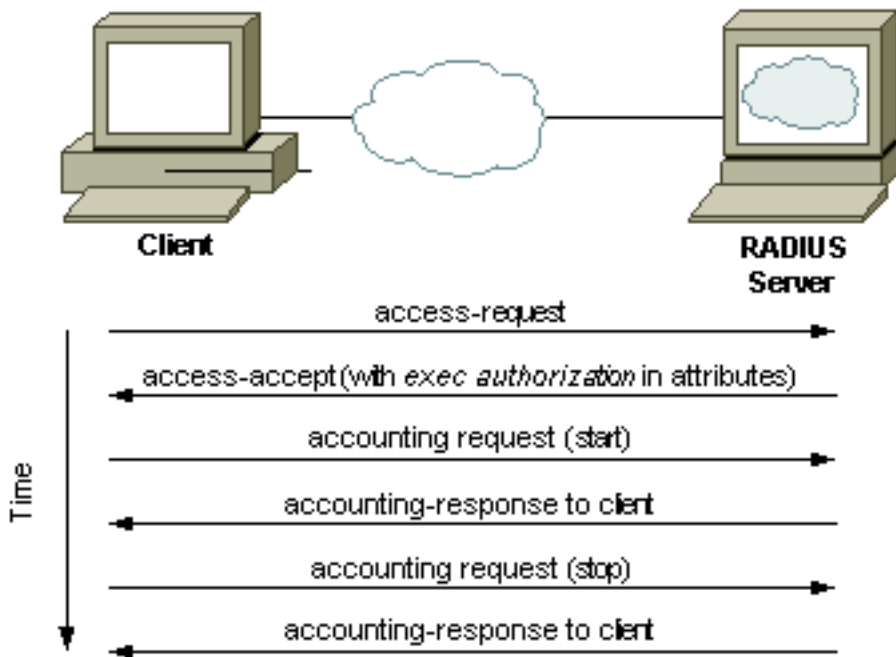
In questo esempio si presume che l'autenticazione di accesso, l'autorizzazione di esecuzione, l'autorizzazione dei comandi, l'accounting di avvio-arresto e l'accounting dei comandi siano implementati con TACACS+ quando un utente si collega in modalità Telnet a un router, esegue un comando e esce dal router:



Esempio di traffico RADIUS

In questo esempio si presume che l'autenticazione di accesso, l'autorizzazione di esecuzione e

l'accounting start-stop in modalità di esecuzione siano implementati con RADIUS quando un utente si connette in modalità Telnet a un router, esegue un comando ed esce dal router (altri servizi di gestione non sono disponibili):



Supporto dispositivo

In questa tabella vengono elencati i supporti TACACS+ e RADIUS AAA per tipo di dispositivo per le piattaforme selezionate. Questa include la versione software in cui è stato aggiunto il supporto. Per ulteriori informazioni, consultare le note di rilascio del prodotto se il prodotto non è presente nell'elenco.

Dispositivo Cisco	Autenticazione TACACS+	Autorizzazione TACACS+	Accounting TACACS+	Autenticazione RADIUS	autorizzazione RADIUS	Accounting RADIUS
Cisco Aironet ¹	12.2(4) JA	12.2(4) JA	12.2(4) JA	tutti gli access point	tutti gli access point	tutti gli access point
Software Cisco IOS ²	10.33	10.33	10.333	11.1.1	11.1.14	11.1.15
Cisco Cache Engine	—	—	—	1.5	1.56	—
Switch Cisco Catalyst	2.2	5.4.1	5.4.1	5.1	5.4.14	5.4.15
Cisco	5.03	5.03	5.03	5.0	5.04	—

CSS 1000 Content Services Switch						
Cisco CSS 1500 Content Services Switch	5.20	5.20	5.20	5.20	5.204	—
Cisco PIX Firewall	4.0	4.07	4.28, 5	4.0	5.27	4.28, 5
Switch Cisco Catalyst 1900/2820	8.x enterprise ⁹	—	—	—	—	—
Switch Cisco Catalyst 2900XL/3500XL	11.2(8)SA6 ¹⁰	11.2(8)SA6 ¹⁰	11.2(8)SA6 ¹⁰	12.0(5)WC5 ¹¹	12.0(5)WC5 ^{11,4}	12.0(5)WC5 ^{11,5}
Cisco VPN 3000 Concentrator ⁶	3.0	3.0	—	2.012	2.0	2.012
Cisco VPN 5000 Concentrator	—	—	—	5,2X ¹²	5,2X ¹²	5,2X ¹

[Note tabella](#)

1. Terminazione dei soli client wireless, non del traffico di gestione in versioni diverse dal software Cisco IOS versione 12.2(4)JA o successive. Nel software Cisco IOS versione 12.2.1(4)JA o successive, è possibile eseguire l'autenticazione sia per la terminazione dei client wireless sia per il traffico di gestione.
2. Per il supporto della piattaforma nel software Cisco IOS, selezionare Feature Navigator (ora obsoleto per [Software Advisor](#) (solo utenti [registrati](#))).
3. L'accounting dei comandi non è implementato fino al software Cisco IOS versione 11.1.6.3.
4. Nessuna autorizzazione per i comandi.
5. Nessun accounting dei comandi.
6. Solo blocco URL, non traffico amministrativo.

7. Autorizzazione per il traffico non VPN attraverso il PIX. **Nota:** versione 5.2 - Supporto dell'elenco degli accessi per l'autorizzazione ACL (Access Control List) RADIUS VSA (Vendor-Specific Attribute) o TACACS+ per il traffico VPN che termina sulla versione 6.1 - Supporto dell'autorizzazione ACL RADIUS 11 per il traffico VPN che termina sulla versione 6.2.2 - Supporto degli ACL scaricabili con autorizzazione RADIUS per il traffico VPN che termina sulla versione 6.2 - Supporto dell'autorizzazione per il traffico di gestione PIX attraverso TACACS+.
8. Rilevamento del traffico non VPN solo attraverso il PIX, non attraverso il traffico di gestione. **Nota:** release 5.2 - Supporto per l'accounting dei pacchetti TCP client VPN tramite PIX.
9. Solo software aziendale.
10. È necessaria una memoria flash da 8 MB per l'immagine.
11. Solo terminazione VPN.

[Informazioni correlate](#)

- [Pagina di supporto RADIUS](#)
- [Documentazione relativa a TACACS+ in IOS](#)
- [Pagina di supporto TACACS/TACACS+](#)
- [RFC \(Requests for Comments\)](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)