# Configurazione del server AAA di base su un server di accesso

## Sommario



## Introduzione

In questo documento viene descritto come configurare l'autenticazione, l'autorizzazione e l'accounting (AAA) su un router Cisco con protocolli Radius o TACACS+.

# Prerequisiti

## Requisiti

Nessun requisito specifico previsto per questo documento.

## Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

## Componenti usati

Per la stesura del documento, è stato usato il software Cisco IOS® versione 12, riga principale.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

# Premesse

Questo documento spiega come configurare l'autenticazione, l'autorizzazione e l'accounting (AAA) su un router Cisco con protocolli Radius o TACACS+. Scopo del documento non è descrivere tutte le funzionalità AAA, ma spiegare i comandi principali e fornire alcuni esempi e alcune linee guida.

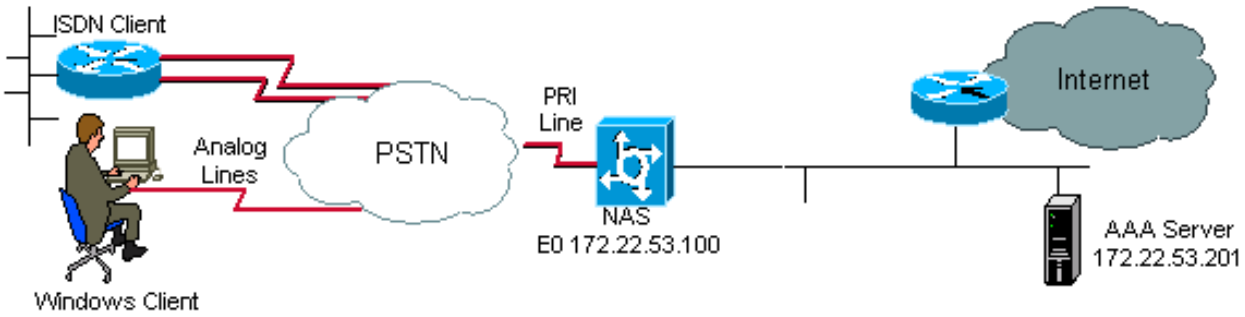
---

Nota: leggere la sezione sulla configurazione generale del server AAA prima di procedere con la configurazione di Cisco IOS. In caso contrario, la configurazione potrebbe non essere corretta e il sistema potrebbe bloccarsi.

---

Per ulteriori informazioni, vedere la guida alla configurazione di autenticazione, autorizzazione e accounting.

## Esempio di rete




Esempio di rete

# Configurazione generale AAA

## Abilita AAA

Per abilitare AAA, è necessario configurare il comando aaa new-model in modalità di configurazione globale.

Nota: finché questo comando non è abilitato, tutti gli altri comandi AAA sono nascosti.

Avviso: il comando aaa new-model applica immediatamente l'autenticazione locale a tutte le righe e interfacce (ad eccezione della riga della console con 0). Se una sessione telnet viene aperta al router dopo l'attivazione di questo comando (o se la connessione scade e deve riconnettersi), l'utente deve essere autenticato con il database locale del router. Si consiglia di definire un nome utente e una password sul server di accesso prima di avviare la configurazione AAA, in modo da non rimanere bloccati sul router. Vedere l'esempio di codice successivo.

<#root>

```
Router(config)#
```

**username xxx password yyy**

Consiglio: prima di configurare i comandi AAA, save la configurazione. È possibile save ridefinire la configurazione solo dopo aver completato la configurazione AAA (e aver verificato che funzioni correttamente). In questo modo è possibile eseguire il ripristino da blocchi imprevisti durante il rollback di qualsiasi modifica con il ricaricamento del router.

## Specificare il server AAA esterno

In una configurazione globale, definire il protocollo di sicurezza da usare con AAA (Radius,

TACACS+). Se non si desidera utilizzare uno di questi due protocolli, è possibile utilizzare il database locale sul router.

Se si usa TACACS+, usare il comando tacacs-server host <indirizzo IP del server AAA> <chiave>.

Se si usa Radius, usare il comando radius-server host <indirizzo IP del server AAA> <chiave>.

### Configurazione server AAA

Sul server AAA, configurare i seguenti parametri:

- Il nome del server di accesso.
- L'indirizzo IP usato dal server di accesso per comunicare con il server AAA.

> Nota: se entrambi i dispositivi si trovano sulla stessa rete Ethernet, per impostazione predefinita il server di accesso utilizza l'indirizzo IP definito sull'interfaccia Ethernet quando invia il pacchetto AAA. Questo problema è importante quando il router ha più interfacce (e quindi più indirizzi).

- La stessa chiave <key> configurata nel server di accesso.

> Nota: la chiave fa distinzione tra maiuscole e minuscole.

- Il protocollo utilizzato dal server di accesso (TACACS+ o Radius).

Per la procedura esatta utilizzata per configurare i parametri precedenti, consultare la documentazione del server AAA in uso. Se il server AAA non è configurato correttamente, le richieste AAA provenienti dal server NAS possono essere ignorate dal server AAA e la connessione potrebbe non riuscire.

Il server AAA deve essere raggiungibile tramite IP dal server di accesso (eseguire un test ping per verificare la connettività).

## Configurazione autenticazione

L'autenticazione verifica gli utenti prima che possano accedere alla rete e ai servizi di rete (che vengono verificati con l'autorizzazione).

Per configurare l'autenticazione AAA:

1. Definire innanzitutto un elenco denominato di metodi di autenticazione (in modalità di configurazione globale).
2. Applicare l'elenco a una o più interfacce (in modalità di configurazione interfaccia).

L'unica eccezione è rappresentata dall'elenco dei metodi predefiniti, denominato default. L'elenco

di metodi predefinito viene applicato automaticamente a tutte le interfacce ad eccezione di quelle per le quali è stato definito in modo esplicito un elenco di metodi denominato. Un elenco di metodi definito sostituisce l'elenco di metodi predefinito.

In questi esempi di autenticazione vengono utilizzate l'autenticazione Radius, di accesso e PPP (Point-to-Point Protocol) per illustrare concetti quali metodi ed elenchi denominati. In tutti gli esempi, TACACS+ può essere sostituito con Radius o con l'autenticazione locale.

Il software Cisco IOS utilizza il primo metodo elencato per autenticare gli utenti. Se il metodo non risponde (indicato da un errore), il software Cisco IOS seleziona il metodo di autenticazione successivo elencato nell'elenco dei metodi. Questo processo continua finché non viene stabilita una comunicazione con un metodo di autenticazione elencato oppure finché tutti i metodi definiti nell'elenco non sono esauriti.

È importante notare che il software Cisco IOS tenta l'autenticazione con il metodo di autenticazione riportato di seguito solo quando non riceve risposta dal metodo precedente. Se l'autenticazione ha esito negativo in qualsiasi momento del ciclo, ovvero se il server AAA o le risposte al database dei nomi utente locali hanno l'obiettivo di negare l'accesso all'utente (indicato da un messaggio di errore), il processo di autenticazione viene interrotto e non vengono tentati altri metodi di autenticazione.

Per consentire l'autenticazione degli utenti, è necessario configurare il nome utente e la password sul server AAA.

## Autenticazione di accesso

È possibile usare il comando aaa authentication login per autenticare gli utenti che vogliono accedere in modalità di esecuzione al server di accesso (tty, vty, console e aux).

Esempio 1: accesso Exec con raggio, quindi locale

<#root>

```
Router(config)#
```

**aaa authentication login default group radius local**

Nel comando precedente:

- L'elenco denominato è quello predefinito (impostazione predefinita).
- Sono disponibili due metodi di autenticazione (group radius e local).

Tutti gli utenti vengono autenticati con il server Radius (il primo metodo). Se il server Radius non risponde, viene utilizzato il database locale del router (il secondo metodo). Per l'autenticazione locale, definire il nome utente e la password:

<#root>

```
Router(config)#
```

**username xxx password yyy**

Poiché viene utilizzato l'elenco predefinito nel comando aaa authentication login, l'autenticazione dell'accesso viene applicata automaticamente a tutte le connessioni di accesso (ad esempio tty, vty, console e aux).

Nota: il server (Radius o TACACS+) non può rispondere a una richiesta di autenticazione AAA inviata dal server di accesso se non è disponibile una connettività IP, se il server di accesso non è definito correttamente sul server AAA o se il server AAA non è definito correttamente sul server di accesso.

Nota: se si utilizza l'esempio precedente senza la parola chiave local, il risultato è:

<#root>

```
Router(config)#
```

**aaa authentication login default group radius**

Nota: se il server AAA non risponde alla richiesta di autenticazione, l'autenticazione non riesce (poiché il router non dispone di un metodo alternativo da provare).

Nota: la parola chiave group consente di raggruppare gli host server correnti. Questa funzione consente all'utente di selezionare un sottoinsieme degli host server configurati e di utilizzarli per un particolare servizio.

Esempio 2: accesso console utilizzato con password di linea

Espandere la configurazione dall'Esempio 1 in modo che l'accesso alla console venga autenticato solo dalla password impostata alla riga con 0.

L'elenco CONSOLE viene definito e quindi applicato alla riga con 0.

Configurazione:

<#root>

```
Router(config)#
```

**aaa authentication login CONSOLE line**

Nel comando precedente:

- L'elenco denominato è CONSOLE.
- Esiste un solo metodo di autenticazione (riga).

Quando si crea un elenco denominato (in questo esempio, CONSOLE), è necessario applicarlo a una riga o a un'interfaccia prima di eseguirlo. Questa operazione viene eseguita con login authentication

comando:

```
<#root>

Router(config)#

line con 0

Router(config-line)#

exec-timeout 0 0

Router(config-line)#

password cisco

Router(config-line)#

login authentication CONSOLE
```

L'elenco CONSOLE sostituisce l'elenco di metodi predefinito predefinito sulla riga con 0. Dopo questa configurazione sulla linea con 0, è necessario immettere la password cisco per poter accedere alla console. L'elenco predefinito è ancora utilizzato nei formati tty, vty e aux.

---

Nota: per autenticare l'accesso alla console con un nome utente e una password locali, utilizzare il codice di esempio riportato di seguito.

---

```
<#root>

Router(config)#

aaa authentication login CONSOLE local
```

In questo caso, è necessario configurare un nome utente e una password nel database locale del router. L'elenco deve essere applicato anche alla linea o all'interfaccia.

Nota: per non eseguire l'autenticazione, utilizzare il codice di esempio riportato di seguito.

```
<#root>

Router(config)#

aaa authentication login CONSOLE none
```

In questo caso, non vi è autenticazione per accedere alla console. L'elenco deve essere applicato anche alla linea o all'interfaccia.

Esempio 3: abilitazione dell'accesso in modalità utilizzata con il server AAA esterno

È possibile eseguire l'autenticazione per ottenere la modalità di abilitazione (privilegio 15).

Configurazione:

```
<#root>

Router(config)#

aaa authentication enable default group radius enable
```

È possibile richiedere solo la password. Il nome utente è $enab15$. È quindi necessario definire il nome utente $enab15$ sul server AAA.

Se il server Radius non risponde, può essere necessario immettere la password di abilitazione configurata localmente sul router.

## Autenticazione PPP

Il comando aaa authentication ppp viene utilizzato per autenticare una connessione PPP. Viene in genere utilizzato per autenticare gli utenti remoti ISDN o analogici che desiderano accedere a Internet o a un ufficio centrale tramite un server di accesso.

Esempio 1: metodo di autenticazione PPP singolo per tutti gli utenti

Il server di accesso dispone di un'interfaccia ISDN configurata per accettare i client remoti PPP. Utilizziamo un dialer rotary-group 0, ma la configurazione può essere effettuata sull'interfaccia principale o sull'interfaccia dialer profile.

Configurazione:

```
<#root>
```

```
Router(config)#
aaa authentication ppp default group radius local
```

Questo comando autentica tutti gli utenti PPP con Radius. Se il server Radius non risponde, viene utilizzato il database locale.

Esempio 2: autenticazione PPP utilizzata con un elenco specifico

Per utilizzare un elenco denominato anziché l'elenco predefinito, configurare i seguenti comandi:

<#root>

```
Router(config)#
aaa authentication ppp ISDN_USER group radius

Router(config)#
interface dialer 0

Router(config-if)#
ppp authentication chap ISDN_USER
```

Nell'esempio, l'elenco è ISDN_USER e il metodo è Radius.

Esempio 3: PPP avviato dalla sessione in modalità carattere

Il server di accesso dispone di una scheda modem interna (Mica, Microcom o Next Port). Si supponga che siano configurati entrambi i comandi aaa authentication login e aaa authentication ppp.

Se un utente modem accede per la prima volta al router con una sessione di esecuzione in modalità carattere (ad esempio, con Finestra terminale dopo la composizione), l'utente viene autenticato su una riga di comando. Per avviare una sessione in modalità pacchetto, gli utenti devono digitare ppp predefinito o ppp. Poiché l'autenticazione PPP è configurata in modo esplicito (con aaa authentication ppp), l'utente viene nuovamente autenticato a livello PPP.

Per evitare questa seconda autenticazione, utilizzare la parola chiave if-needed:

<#root>

```
Router(config)#
aaa authentication login default group radius local
Router(config)#
```

```
aaa authentication ppp default group radius local if-needed
```

Nota: se il client avvia direttamente una sessione PPP, l'autenticazione PPP viene eseguita direttamente poiché non è disponibile l'accesso al server di accesso.

# Configura autorizzazione

L'autorizzazione è il processo mediante il quale è possibile controllare le operazioni che un utente può eseguire.

L'autorizzazione AAA ha le stesse regole dell'autenticazione:

1. Definire innanzitutto un elenco denominato di metodi di autorizzazione.
2. Applicare quindi l'elenco a una o più interfacce (ad eccezione dell'elenco dei metodi predefiniti).
3. Viene utilizzato il primo metodo elencato. Se non risponde, viene utilizzato il secondo, e così via.

Gli elenchi di metodi sono specifici del tipo di autorizzazione richiesto. Nel documento vengono illustrati in particolare i tipi di autorizzazione Exec e Network.

Per ulteriori informazioni sugli altri tipi di autorizzazione, consultare la guida alla configurazione della sicurezza di Cisco IOS.

## Autorizzazione Exec

Il comando aaa authorization exec determina se l'utente è autorizzato a eseguire una shell di esecuzione. Questa funzionalità può restituire le informazioni del profilo utente, ad esempio le informazioni sul comando automatico, il timeout di inattività, il timeout della sessione, l'elenco degli accessi e i privilegi, nonché altri fattori per utente.

L'autorizzazione di esecuzione viene eseguita solo sulle righe vty e tty.

Nell'esempio seguente viene utilizzato il valore Radius.

Esempio 1: Metodi di autenticazione Exec uguali per tutti gli utenti

Quando viene autenticato con:

<#root>

```
Router(config)#
```

```
aaa authentication login default group radius local
```

Tutti gli utenti che desiderano accedere al server di accesso devono essere autorizzati con Radius (primo metodo) o database locale (secondo metodo).

Configurazione:

```
<#root>

Router(config)#

aaa authorization exec default group radius local
```

Nota: sul server AAA, è necessario selezionare Service-Type=1 (login).

Nota: in questo esempio, se la parola chiave local non è inclusa e il server AAA non risponde, l'autorizzazione non è possibile e la connessione può non riuscire.

Nota: negli esempi 2 e 3 successivi, non è necessario aggiungere alcun comando sul router. È sufficiente configurare il profilo sul server di accesso.

Esempio 2: assegnazione di livelli di privilegi di esecuzione dal server AAA

In base all'esempio 1, configurare la successiva coppia Cisco AV sul server AAA in modo che un utente possa accedere al server di accesso e accedere direttamente alla modalità di abilitazione:

```
shell:priv-lvl=15
```

L'utente può passare direttamente alla modalità di abilitazione.

Nota: se il primo metodo non risponde, viene utilizzato il database locale. Tuttavia, l'utente non può accedere direttamente alla modalità di abilitazione, ma deve immettere il comando enable e fornire la password di abilitazione.

Esempio 3: assegnazione del timeout di inattività dal server AAA

Per configurare un timeout di inattività (in modo che la sessione venga disconnessa in caso di assenza di traffico dopo il timeout di inattività), utilizzare l'attributo IETF Radius 28: Idle-Timeout nel profilo utente.

## Autorizzazione di rete

OSPF (Open Shortest Path First) aaa authorization network esegue l'autorizzazione per tutte le richieste di servizio relative alla rete, ad esempio PPP, SLIP e ARAP. In questa sezione vengono illustrati i protocolli PPP più comunemente utilizzati.

Il server AAA verifica se è consentita una sessione PPP da parte del client. Inoltre, le opzioni PPP possono essere richieste dal client: callback, compressione, indirizzo IP e così via. Queste opzioni devono essere configurate sul profilo utente sul server AAA. Inoltre, per un client specifico, il profilo AAA può contenere il timeout di inattività, l'elenco degli accessi e altri attributi per utente, che possono essere scaricati dal software Cisco IOS e applicati al client.

Negli esempi seguenti viene illustrata l'autorizzazione con Radius.

Esempio 1: Metodi di autorizzazione di rete uguali per tutti gli utenti

Il server di accesso viene utilizzato per accettare connessioni remote PPP.

Gli utenti vengono autenticati (come configurato in precedenza) con:

```
<#root>

Router(config)#

aaa authentication ppp default group radius local
```

Utilizzare il comando successivo per autorizzare gli utenti:

```
<#root>

Router(config)#

aaa authorization network default group radius local
```

---

Nota: sul server AAA configurare: Service-Type=7 (framed) e Framed-Protocol=PPP.

---

Esempio 2: applicazione di attributi specifici dell'utente

È possibile utilizzare il server AAA per assegnare gli attributi per utente, ad esempio l'indirizzo IP, il numero di richiamata, il valore di timeout di inattività della connessione telefonica o l'elenco degli accessi e così via. In questa implementazione, il NAS scarica gli attributi appropriati dal profilo utente del server AAA.

Esempio 3: autorizzazione PPP con un elenco specifico

Analogamente all'autenticazione, configurare un nome di elenco anziché quello predefinito:

<#root>

```
Router(config)#
aaa authorization network ISDN_USER group radius local
```

Quindi, applicare questo elenco all'interfaccia:

<#root>

```
  Router(config)#
interface dialer 0

  Router(config-if)#
ppp authorization ISDN_USER
```

# Configurazione accounting

La funzione di contabilità AAA consente di tenere traccia dei servizi a cui gli utenti accedono e della quantità di risorse di rete che utilizzano.

La contabilità AAA prevede le stesse regole di autenticazione e autorizzazione:

1. È innanzitutto necessario definire un elenco denominato di metodi contabili.
2. Applicare quindi l'elenco a una o più interfacce (ad eccezione dell'elenco dei metodi predefiniti).
3. Viene utilizzato il primo metodo elencato, se non risponde, il secondo viene utilizzato e così via.

- L'accounting di rete fornisce informazioni per tutte le sessioni PPP, Slip e AppleTalk Remote Access Protocol (ARAP): numero di pacchetti, numero di ottetti, ora della sessione, ora di inizio e di fine.
- L'accounting di esecuzione fornisce informazioni sulle sessioni terminale di esecuzione utente (ad esempio una sessione telnet) del server di accesso alla rete: ora di sessione, ora di avvio e ora di arresto.

Negli esempi seguenti viene illustrato come inviare le informazioni al server AAA.

## Esempi di configurazione dell'accounting

Esempio 1: Genera record contabili di avvio e di arresto

Per ogni sessione PPP remota, le informazioni di accounting vengono inviate al server AAA dopo

l'autenticazione del client e dopo la disconnessione con la parola chiave start-stop.

<#root>

```
Router(config)#
```

```
aaa accounting network default start-stop group radius local
```

Esempio 2: Genera solo record contabili interrotti

Se le informazioni di accounting devono essere inviate solo dopo la disconnessione di un client, utilizzare la parola chiave stop e configurare la riga successiva:

<#root>

```
Router(config)#
```

```
aaa accounting network default stop group radius local
```

Esempio 3: generazione di record di risorse per errori di autenticazione e negoziazione

Fino a questo punto, l'accounting AAA fornisce il supporto di record di avvio e arresto per le chiamate che hanno superato l'autenticazione utente.

Se l'autenticazione o la negoziazione PPP ha esito negativo, non vi è alcun record di autenticazione.

La soluzione consiste nell'utilizzare la risorsa AAA per interrompere l'accounting:

<#root>

```
Router(config)#
```

```
aaa accounting send stop-record authentication failure
```

Al server AAA viene inviato un record di interruzione.

Esempio 4: Abilita contabilità completa delle risorse

Per abilitare la contabilità completa delle risorse, che genera sia un record iniziale durante l'impostazione della chiamata che un record finale alla terminazione della chiamata, configurare:

<#root>

```
Router(config)#
aaa accounting resource start-stop
```

Questo comando è stato introdotto nel software Cisco IOS versione 12.1(3)T.

Con questo comando, un record di impostazione e disconnessione di chiamata start-stop accounting registra lo stato della connessione delle risorse al dispositivo. Un record di accounting start-stop per l'autenticazione degli utenti separato tiene traccia dello stato di avanzamento della gestione degli utenti. Questi due set di record contabili sono collegati a un ID sessione univoco per la chiamata.

## Informazioni correlate

- Supporto tecnico Cisco e download

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).