Configurazione di CSU per UNIX (Solaris)

Sommario

Introduzione

Il software Cisco Secure ACS for UNIX (CSU) contribuisce a garantire la sicurezza della rete e a tenere traccia delle attività degli utenti che si connettono correttamente alla rete. La CSU opera come server TACACS+ o RADIUS e utilizza l'autenticazione, l'autorizzazione e l'accounting (AAA) per garantire la sicurezza della rete.

CSU supporta le seguenti opzioni di database per archiviare i profili utente e di gruppo e le informazioni di accounting:

- SQLAnywhere (inclusa con CSU).Questa versione di Sybase SQLAnywhere non dispone del supporto client/server. Tuttavia, è ottimizzato per eseguire i servizi AAA essenziali con CSU.**Attenzione:** l'opzione di database SQLAnywhere non supporta i database di profili con più di 5.000 utenti, la replica delle informazioni sui profili tra i siti di database o la funzionalità Cisco Secure Distribute Session Manager (DSM).
- Oracle o Sybase Relational Database Management System (RDBMS).Per supportare i database di profilo Cisco Secure con 5.000 o più utenti, la replica di database o la funzionalità Cisco Secure DSM, è necessario preinstallare un RDBMS Oracle (versione 7.3.2, 7.3.3 o 8.0.3) o Sybase SQL Server (versione 11) per conservare le informazioni del profilo Cisco Secure. La replica del database richiede un'ulteriore configurazione RDBMS dopo il

completamento dell'installazione di Cisco Secure.
- Aggiornamento di un database esistente da una versione precedente (2.x) di CSU.Se si esegue l'aggiornamento da una versione precedente di Cisco Secure 2.x, il programma di installazione di Cisco Secure aggiorna automaticamente il database dei profili in modo che sia compatibile con CSU 2.3 per UNIX.
- Importazione di un database dei profili esistente.Èpossibile convertire i database dei profili TACACS+ o RADIUS freeware esistenti o i file sequenziali da utilizzare con questa versione della CSU.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni di questo documento si basano su Cisco Secure ACS 2.3 per UNIX.

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.

Convenzioni

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

Configurazione CSU

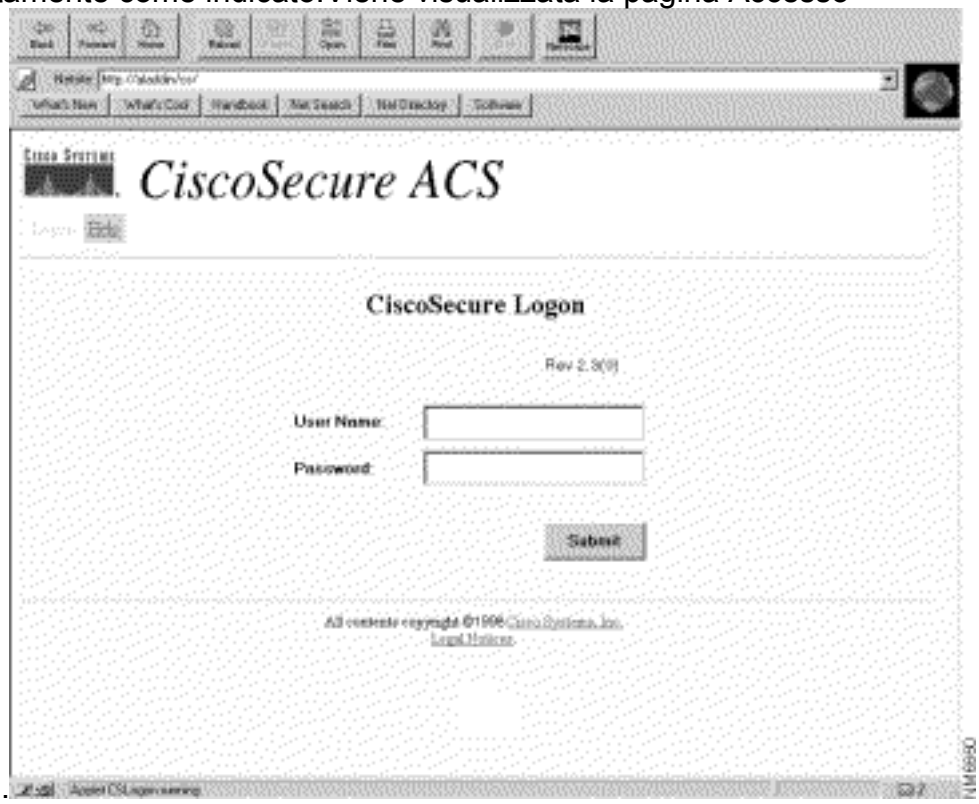
Utilizzare le seguenti procedure per configurare la CSU.

Avviare Cisco Secure Administrator Interface

Utilizzare questa procedura per accedere a Cisco Secure Administrator.

1. Da qualsiasi workstation con una connessione Web ad ACS, avviare il browser Web.
2. Immettere uno degli URL seguenti per il sito Web Cisco Secure Administrator:Se la funzione di livello socket di sicurezza del browser non è attivata, immettere:
   `http://your_server/cs`
   dove server è il nome host (o il nome di dominio completo (FQDN), se il nome host e FQDN sono diversi) della stazione SPARC in cui è stata installata la CSU. È inoltre possibile sostituire il server con l'indirizzo IP della stazione SPARCstation.Se la funzione del livello del socket di sicurezza del browser è attivata, specificare "https" anziché "http" come protocollo di trasmissione ipertestuale. Inserire:
   `https://your_server/cs`
   dove server è il nome host (o FQDN, se il nome host e FQDN sono diversi) della stazione

SPARC in cui è stata installata la CSU. È inoltre possibile sostituire il server con l'indirizzo IP della stazione SPARCstation.**Nota: per** gli URL e i nomi di server viene fatta distinzione tra maiuscole e minuscole. Devono essere digitati con lettere maiuscole e minuscole esattamente come indicato.Viene visualizzata la pagina Accesso CSU.

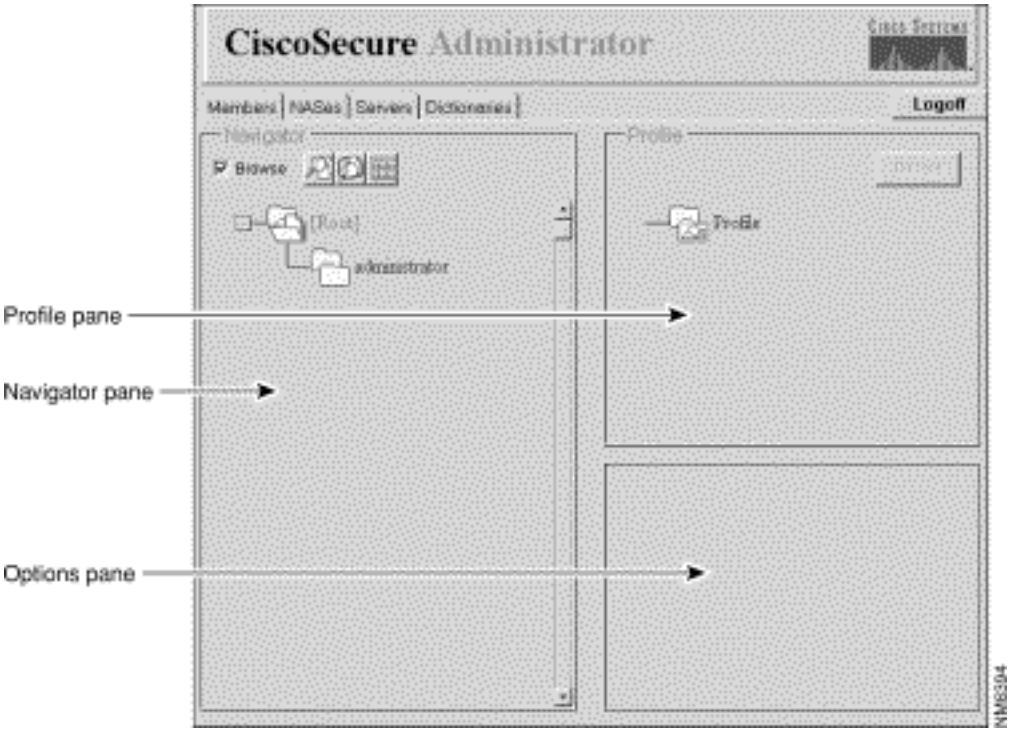


3. Immettere il nome utente e la password. Fare clic su **Invia**.**Nota:** il nome utente predefinito iniziale è "superuser". La password predefinita iniziale è "changeme". Dopo l'accesso iniziale, è necessario modificare immediatamente il nome utente e la password per garantire la massima protezione.Una volta effettuato l'accesso, viene visualizzata la pagina principale CSU con la barra dei menu principale nella parte superiore. La pagina del menu principale CSU viene visualizzata solo se l'utente fornisce un nome e una password con privilegi di amministratore. Se l'utente fornisce un nome e una password che dispongono solo di privilegi a livello utente, verrà visualizzata una schermata diversa.

Avvia il programma di configurazione avanzata

Avviare il programma Cisco Secure Administrator Advanced Configuration basato su Java da una delle pagine Web di CSU Administrator. Dalla barra dei menu dell'interfaccia Web CSU, fare clic su **Advanced** (Avanzate), quindi fare di nuovo clic su **Advanced** (Avanzate).

Viene visualizzato il programma Cisco Secure Administrator Advanced Configuration. Il caricamento potrebbe richiedere alcuni minuti.

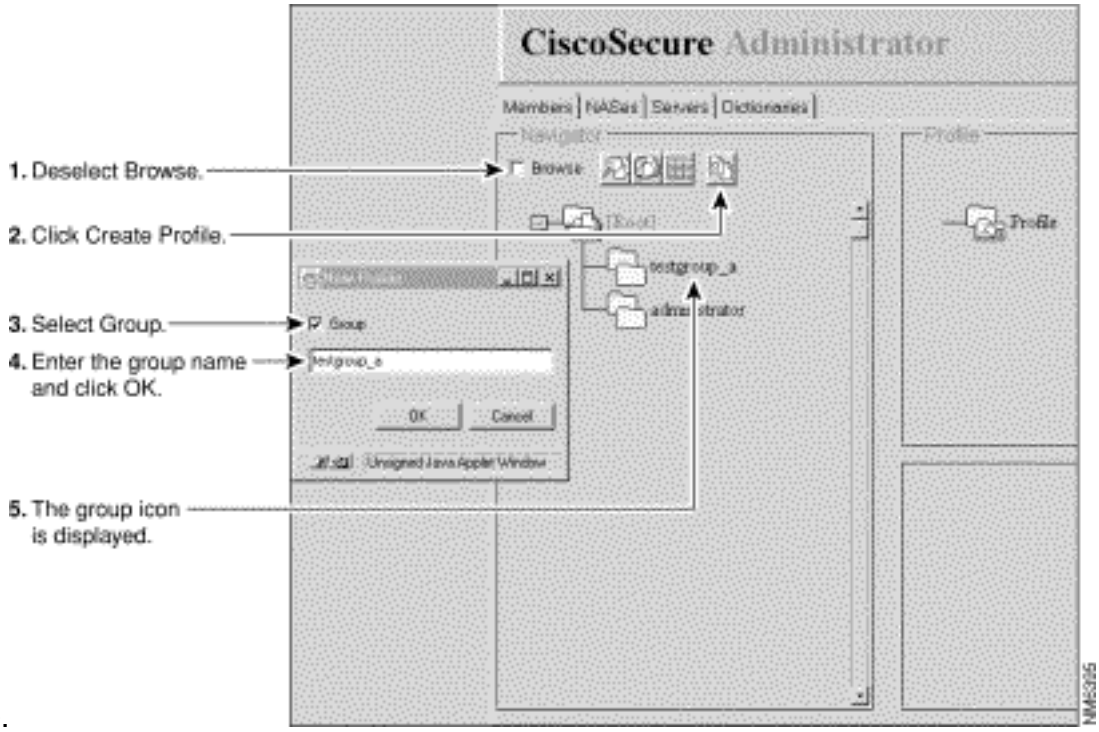


Crea un profilo di gruppo

Utilizzare il programma Cisco Secure Administrator Advanced Configuration per creare e configurare i profili di gruppo. Cisco consiglia di creare profili di gruppo per configurare requisiti AAA dettagliati per un elevato numero di utenti simili. Dopo aver definito il profilo del gruppo, utilizzare la pagina Web CSU Add a User per aggiungere rapidamente i profili utente al profilo del gruppo. I requisiti avanzati configurati per il gruppo si applicano a ogni utente membro.

Utilizzare questa procedura per creare un profilo di gruppo.

1. Nel programma Cisco Secure Administrator Advanced Configuration, selezionare la scheda **Membri**. Nel riquadro del Navigator, deselezionare la casella di controllo **Sfoglia**. Viene visualizzata l'icona Crea nuovo profilo.
2. Nel riquadro del Navigator, effettuare una delle seguenti operazioni:Per creare un profilo di gruppo senza elementi padre, individuare e fare clic sull'icona della cartella [**Root**].Per creare il profilo di gruppo come figlio di un altro profilo di gruppo, individuare il gruppo che si desidera impostare come padre e fare clic su di esso.Se il gruppo padre è un gruppo figlio, fare clic sulla cartella del gruppo padre per visualizzarlo.
3. Fare clic su **Crea nuovo profilo**. Verrà visualizzata la finestra di dialogo Nuovo profilo.
4. Selezionare la casella di controllo **Gruppo**, digitare il nome del gruppo che si desidera creare e fare clic su **OK**. Il nuovo gruppo viene visualizzato nella struttura.
5. Dopo aver creato il profilo di gruppo, assegnare gli attributi TACACS+ o RADIUS per configurare proprietà AAA



specifiche.

Creazione di un profilo utente in modalità di configurazione avanzata

Utilizzare la modalità di configurazione avanzata di Cisco Secure Administrator per creare e configurare un profilo utente. È possibile eseguire questa operazione per personalizzare gli attributi relativi all'autorizzazione e all'accounting del profilo utente in modo più dettagliato di quanto sia possibile nella pagina Aggiungi utente.

Per creare un profilo utente, attenersi alla procedura descritta di seguito.

1. Nel programma Cisco Secure Administrator Advanced Configuration, selezionare la scheda **Membri**. Nel riquadro del Navigator, individuare e deselezionare **Sfoglia**. Viene visualizzata l'icona Crea nuovo profilo.
2. Nel riquadro del Navigator, effettuare una delle seguenti operazioni:Individuare e fare clic sul gruppo a cui appartiene l'utente.Se non si desidera che l'utente appartenga a un gruppo, fare clic sull'icona della cartella [**Root**].
3. Fare clic su **Crea profilo**. Verrà visualizzata la finestra di dialogo Nuovo profilo.
4. Assicurarsi che la casella di controllo **Gruppo** sia deselezionata.
5. Immettere il nome dell'utente che si desidera creare e fare clic su **OK**. Il nuovo utente viene visualizzato nella struttura.
6. Dopo aver creato il profilo utente, assegnare gli attributi TACACS+ o RADIUS specifici per configurare le proprietà AAA specifiche:Per assegnare i profili TACACS+ al profilo utente, vedere Assegnazione degli attributi TACACS+ a un gruppo o a un profilo utente.Per assegnare profili RADIUS al profilo utente, vedere Assegnare attributi RADIUS a un gruppo o a un profilo utente.

Strategie per applicare gli attributi

Usare la funzionalità CSU group profile e gli attributi TACACS+ e RADIUS per implementare l'autenticazione e l'autorizzazione degli utenti della rete tramite CSU.

Attributi del piano per gruppi e utenti

La funzionalità Group Profile della CSU consente di definire un insieme comune di requisiti AAA per un numero elevato di utenti.

Èpossibile assegnare un set di valori degli attributi TACACS+ o RADIUS a un profilo di gruppo. I valori di attributo assegnati al gruppo si applicano a tutti gli utenti che sono membri o che sono stati aggiunti come membri di tale gruppo.

Utilizzo efficace della feature di profilo di gruppo

Per configurare la CSU in modo da gestire un numero elevato di utenti e vari tipi di utenti con requisiti AAA complessi, Cisco consiglia di utilizzare le funzionalità del programma di configurazione avanzata di Cisco Secure Administrator per creare e configurare i profili di gruppo.

Il profilo del gruppo deve contenere tutti gli attributi non specifici dell'utente. Questo significa in genere tutti gli attributi ad eccezione della password. È quindi possibile utilizzare la pagina Aggiungi utente di Cisco Secure Administrator per creare profili utente semplici con attributi di password e assegnare tali profili utente al profilo di gruppo appropriato. Le funzioni e i valori degli attributi definiti per un particolare gruppo vengono quindi applicati agli utenti membri.

Gruppi padre e gruppi figlio

Èpossibile creare una gerarchia di gruppi. All'interno di un profilo di gruppo è possibile creare profili di gruppo figlio. I valori degli attributi assegnati al profilo del gruppo padre sono valori predefiniti per i profili del gruppo figlio.

Amministrazione a livello di gruppo

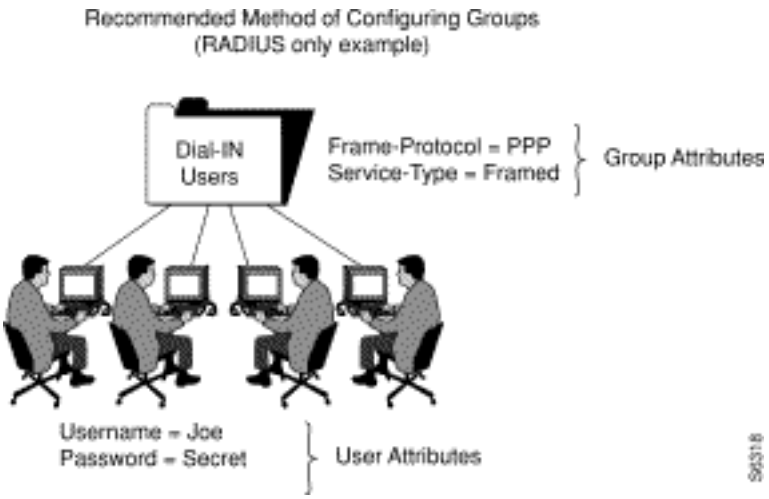
Un amministratore di sistema Cisco Secure può assegnare a singoli utenti Cisco Secure lo stato di amministratore di gruppo. Lo stato Amministratore gruppo consente ai singoli utenti di amministrare i profili dei gruppi figlio e i profili utente subordinati al gruppo. Non consente tuttavia di amministrare gruppi o utenti che non rientrano nella gerarchia del gruppo. In questo modo, l'amministratore di sistema assegna il compito di amministrare una rete di grandi dimensioni ad altri individui senza concedere a ciascuno di essi la stessa autorità.

Attributi definiti per singoli utenti

Cisco consiglia di assegnare ai singoli utenti valori di autenticazione di base univoci per l'utente, ad esempio attributi che definiscono il nome utente, la password, il tipo di password e il privilegio Web. Assegnare i valori dell'attributo di autenticazione di base agli utenti tramite le pagine Modifica utente o Aggiungi utente della CSU.

Attributi da definire per i profili di gruppo

Cisco consiglia di definire gli attributi relativi alla qualifica, all'autorizzazione e alla contabilità a livello di gruppo.



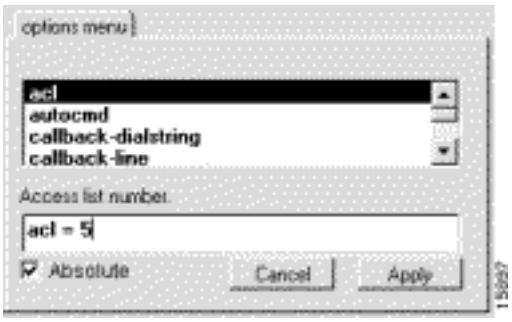
In questo esempio, al profilo di gruppo denominato "Dial-In Users" vengono assegnate le coppie attributo-valore Frame-Protocol=PPP e Service-Type=Framed.

Informazioni sugli attributi assoluti

A un sottoinsieme degli attributi TACACS+ e RADIUS nella CSU può essere assegnato lo stato assoluto a livello di profilo del gruppo. Un valore attributo abilitato per lo stato assoluto a livello di profilo di gruppo sostituisce qualsiasi valore attributo in conflitto a livello di profilo di gruppo figlio o di profilo utente membro.

Nelle reti a più livelli con diversi livelli di amministratori di gruppo, gli attributi assoluti consentono a un amministratore di sistema di impostare valori di attributi di gruppo selezionati che gli amministratori di gruppo ai livelli inferiori non possono ignorare.

Gli attributi a cui è possibile assegnare uno stato assoluto visualizzano una casella di controllo Assoluto nella casella Attributi del programma Cisco Secure Administrator Advanced Configuration. Selezionare la casella di controllo per attivare lo stato assoluto.



È possibile che i valori degli attributi di gruppo e i valori degli attributi utente siano in conflitto?

La risoluzione dei conflitti tra i valori degli attributi assegnati ai profili del gruppo padre, ai profili del gruppo figlio e ai profili utente membro dipende dal fatto che i valori degli attributi siano assoluti e che si tratti di attributi TACACS+ o RADIUS:

- I valori degli attributi TACACS+ o RADIUS assegnati a un profilo di gruppo con stato assoluto sostituiscono i valori degli attributi in conflitto impostati a livello di gruppo figlio o di profilo utente.
- Se lo stato assoluto di un valore dell'attributo TACACS+ non è abilitato a livello di profilo del gruppo, viene sostituito da qualsiasi valore dell'attributo in conflitto impostato a livello di profilo

utente o di gruppo figlio.
- Se lo stato assoluto di un valore di attributo RADIUS non è abilitato a livello di gruppo padre, qualsiasi valore di attributo in conflitto impostato a livello di gruppo figlio produce un risultato imprevedibile. Quando si definiscono i valori degli attributi RADIUS per un gruppo e i relativi utenti membri, evitare di assegnare lo stesso attributo sia al profilo utente che a quello di gruppo.

Utilizzare le opzioni Proibisci e Autorizza

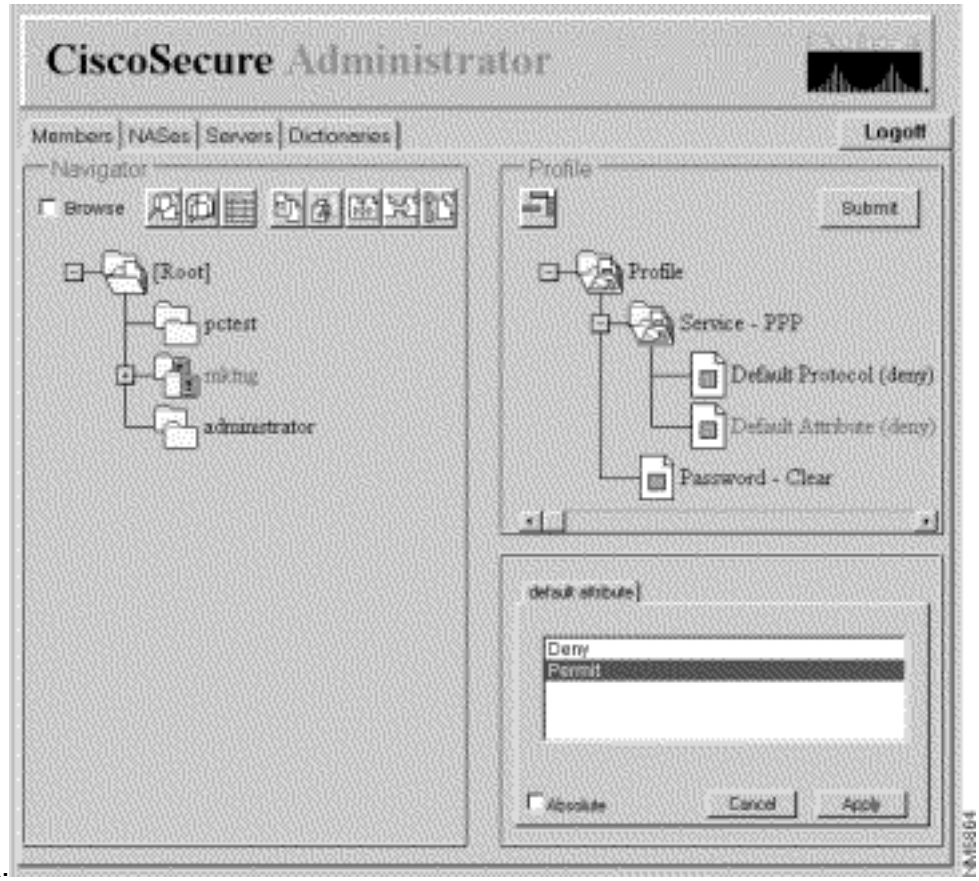
Per TACACS+, ignorare la disponibilità dei valori del servizio ereditati inserendo il prefisso **hibit** o **allow** nella specifica del servizio con la parola chiave **hibit** or **allow**. La parola chiave **allow** consente di specificare servizi. La parola chiave **hibit** disattiva i servizi specificati. L'uso congiunto di queste parole chiave consente di creare configurazioni "tutto tranne". Ad esempio, questa configurazione consente l'accesso da tutti i servizi tranne X.25:

```
default service = permit
prohibit service = x25
```

Assegnazione di attributi TACACS+ a un profilo utente o di gruppo

Per assegnare servizi e attributi TACACS+ specifici a un profilo utente o di gruppo, attenersi alla seguente procedura:

1. Nel programma Cisco Secure Administrator Advanced Configuration, selezionare la scheda **Membri**. Nel riquadro del Navigator, fare clic sull'icona del gruppo o del profilo utente a cui sono assegnati gli attributi TACACS+.
2. Se necessario, nel riquadro Profilo fare clic sull'icona **Profilo** per espanderla.Nella finestra in basso a destra dello schermo viene visualizzato un elenco o una finestra di dialogo contenente gli attributi applicabili al profilo o al servizio selezionato. Le informazioni in questa finestra cambiano in base al profilo o al servizio selezionato nel riquadro Profilo.
3. Fare clic sul servizio o sul protocollo che si desidera aggiungere e quindi su **Applica**. Il servizio viene aggiunto al profilo.
4. Inserire o selezionare il testo necessario nella finestra Attributo.Le voci valide sono spiegate nella sezione Strategie per l'applicazione degli attributi della Guida di riferimento di CSU 2.3 for UNIX.**Nota:** se si assegna un valore di attributo a livello di profilo di gruppo e l'attributo specificato visualizza una casella di controllo **Assoluto**, selezionare tale casella di controllo per assegnare il valore allo stato assoluto. Uno stato assoluto assegnato a un valore non può essere sostituito da valori concorrenti assegnati a livello di profilo di gruppo subordinato o di profilo utente.
5. Ripetere i passaggi da 1 a 1 per ogni servizio o protocollo aggiuntivo da aggiungere.
6. Una volta apportate tutte le modifiche, fare clic su

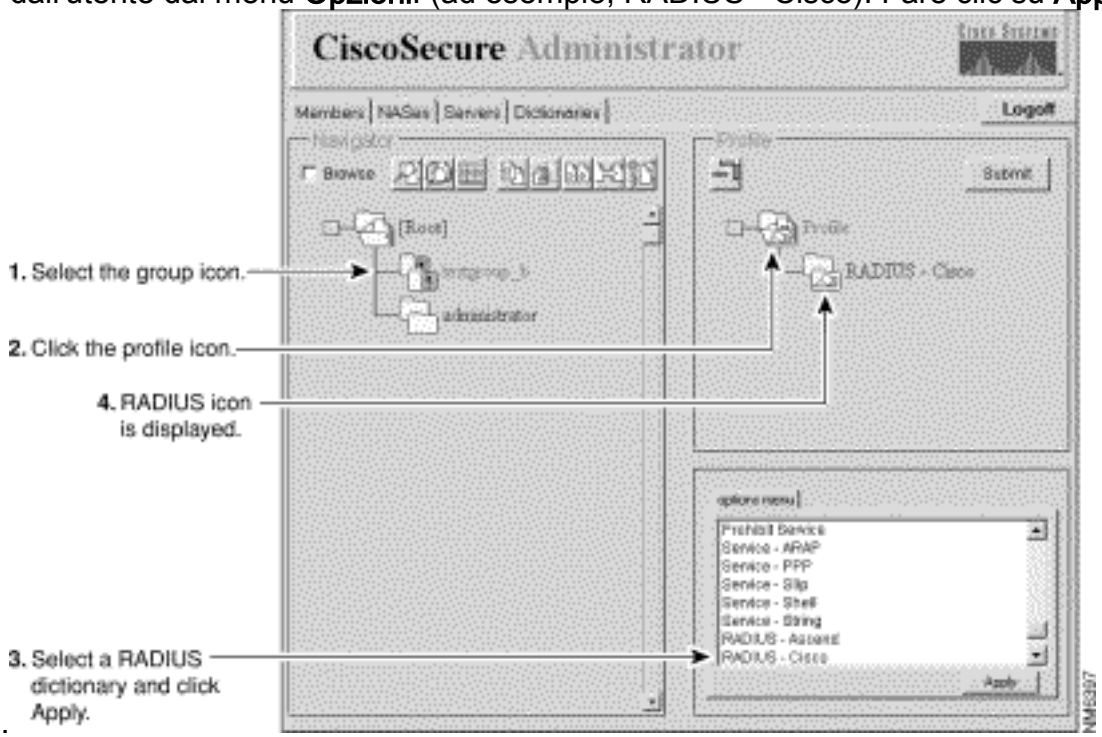


Invia.

Assegnare attributi RADIUS a un gruppo o a un profilo utente

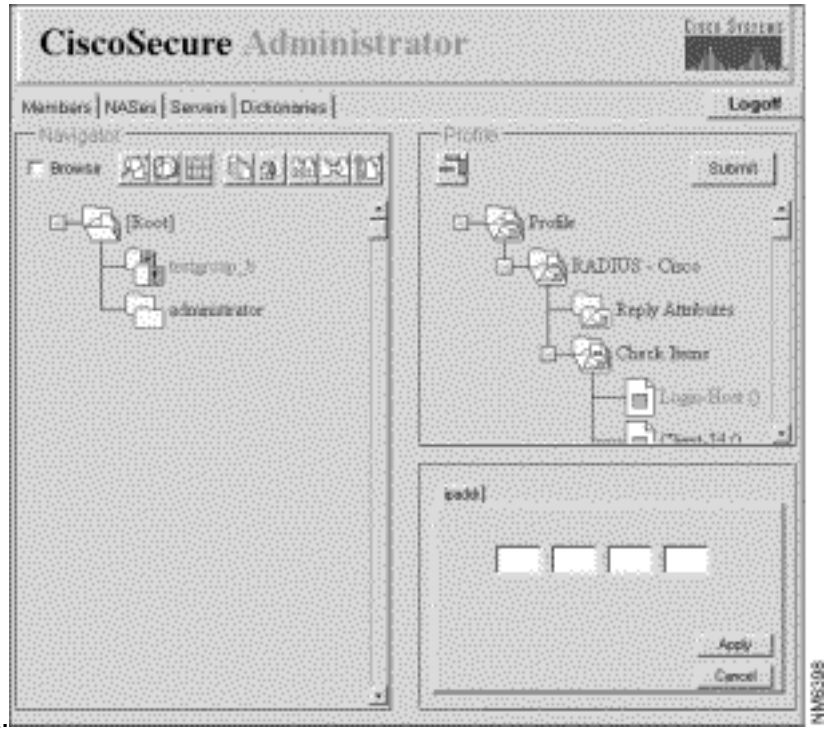
Per assegnare attributi RADIUS specifici a un gruppo o a un profilo utente:

1. Assegnare un dizionario RADIUS al profilo del gruppo:Nella pagina Membri del programma Configurazione avanzata di Cisco Secure Administrator, fare clic sull'icona **Gruppo** o **Utente**, quindi fare clic sull'icona **Profilo** nel riquadro Profili. Nel riquadro Attributi viene visualizzato il menu Opzioni.Scegliere il nome del dizionario RADIUS che si desidera venga utilizzato dal gruppo o dall'utente dal menu **Opzioni**. (ad esempio, RADIUS - Cisco). Fare clic su **Apply** (Applica).



2. Aggiungere gli elementi di controllo e gli attributi di risposta richiesti al profilo RADIUS:**Nota:** gli elementi di controllo sono attributi necessari per l'autenticazione, ad esempio ID utente e password. Gli attributi di risposta sono attributi inviati al server di accesso alla rete (NAS) dopo che il profilo ha superato la procedura di autenticazione, ad esempio Framed-Protocol. Per elenchi e spiegazioni sugli elementi di controllo e gli attributi di risposta, fare riferimento a Radius Attribute-Value Pairs and Dictionary Management nella guida di riferimento CSU 2.3 for UNIX.Nella finestra Profilo, fare clic sull'icona della cartella RADIUS - nomedizionario. Per espandere la cartella RADIUS, è probabilmente necessario fare clic sul simbolo + del profilo. Le opzioni Controlla articoli e Attributi risposta vengono visualizzate nella finestra Gruppo di attributi.Per utilizzare uno o più di questi attributi, fare clic sugli attributi che si desidera utilizzare, quindi fare clic su **Applica**. È possibile aggiungere più di un attributo alla volta.Fare clic sul simbolo **+** per il nome del dizionario RADIUS per espandere la cartella.**Nota:** se si seleziona l'opzione RADIUS-Cisco11.3, accertarsi che il software Cisco IOS® versione 11.3.3(T) o successive sia installato sui NAS di connessione e aggiungere nuove righe di comando alle configurazioni NAS. Fare riferimento alla sezione relativa all'attivazione completa del dizionario RADIUS-Cisco11.3 nella Guida di riferimento di CSU 2.3 for UNIX.
3. Specificare i valori per gli elementi di controllo e gli attributi di risposta aggiunti:**Attenzione:** per il protocollo RADIUS, l'ereditarietà è additiva anziché gerarchica. (Il protocollo TACACS+ utilizza l'ereditarietà gerarchica). Ad esempio, se si assegnano gli stessi attributi di risposta sia al profilo utente che al profilo di gruppo, l'autorizzazione ha esito negativo perché il server NAS riceve il doppio degli attributi. Non ha senso degli attributi di risposta. Non assegnare lo stesso elemento di controllo o attributo di risposta sia al profilo di gruppo che a quello utente.Fare clic su **Controlla elementi** o su **Attributi risposta** oppure fare clic su entrambi. Nella finestra in basso a destra viene visualizzato un elenco dei valori degli elementi di controllo e degli attributi di risposta applicabili. Fare clic sul simbolo **+** per espandere la cartella.Fare clic sui valori che si desidera assegnare, quindi fare clic su **Applica**. Per ulteriori informazioni sui valori, vedere RADIUS Attribute-Value Pairs and Dictionary Management nella Guida di riferimento di CSU 2.3 for UNIX.**Nota:** se si assegna un valore attributo a livello di profilo di gruppo e l'attributo specificato visualizza una casella di controllo Assoluto, selezionare tale casella di controllo per assegnare il valore allo stato assoluto. Un valore assegnato a uno stato assoluto non può essere sostituito da valori concorrenti assegnati a livello di profilo di gruppo subordinato o di profilo utente.Dopo aver apportato le modifiche

desiderate, fare clic su **Invia**.



4. Per utilizzare uno o più di questi attributi, fare clic sugli attributi che si desidera utilizzare, quindi fare clic su **Applica**. È possibile applicare più di un attributo alla volta.

Assegnazione dei livelli di privilegio del controllo di accesso

L'amministratore degli utenti avanzati utilizza l'attributo privilegio Web per assegnare un livello di privilegio di controllo di accesso agli utenti Cisco Secure.

1. Nel programma Configurazione avanzata di Cisco Secure Administrator fare clic sull'utente a cui si desidera assegnare il privilegio di controllo dell'accesso, quindi fare clic sull'icona Profilo nel riquadro Profili.
2. Scegliere **Privilegio Web** dal menu Opzioni e selezionare uno di questi valori.**0** - Nega all'utente qualsiasi privilegio di controllo dell'accesso che includa la possibilità di modificare la password Cisco Secure dell'utente.**1** - Concede all'utente l'accesso alla pagina Web CSUser. Ciò consente agli utenti Cisco Secure di modificare le proprie password Cisco Secure. Per ulteriori informazioni su come modificare le password, vedere Funzioni a livello utente (modifica di una password) in Gestione utenti semplici e ACS.**12** - Concede i privilegi di amministratore del gruppo di utenti.**15** - Concede i privilegi di amministratore di sistema dell'utente.**Nota:** se si seleziona un'opzione di privilegio Web diversa da 0, è necessario specificare anche una password. Per soddisfare il requisito relativo alla password per il privilegio Web, è sufficiente uno spazio vuoto.

Avvia e arresta CSU

In genere, la CSU viene avviata automaticamente all'avvio o al riavvio della stazione SPARCstation in cui è installata. Tuttavia, è possibile avviare CSU manualmente o spegnerlo senza chiudere l'intera SPARCStation.

Accedere come [Root] alla SPARCStation su cui è stato installato CSU.

Per avviare manualmente CSU, digitare:

```
# /etc/rc2.d/S80CiscoSecure
```

Per arrestare manualmente la CSU, digitare:

```
# /etc/rc0.d/K80CiscoSecure
```

Verifica

Attualmente non è disponibile una procedura di verifica per questa configurazione.

Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.

Informazioni correlate

- Pagina di supporto di Cisco Secure ACS per UNIX
- Pagina di supporto TACACS+
- Pagina di supporto RADIUS
- RFC (Requests for Comments)
- Documentazione e supporto tecnico – Cisco Systems