Come assegnare i livelli di privilegio con TACACS+ e RADIUS

Sommario

Introduzione

Questo documento spiega come modificare il livello di privilegi per alcuni comandi e fornisce un esempio con alcune parti di configurazioni di esempio per un router e i server TACACS+ e RADIUS.

Prerequisiti

Requisiti

I lettori di questo documento devono conoscere i livelli di privilegio su un router.

Per impostazione predefinita, il router dispone di tre livelli di privilegi.

- livello di privilegio 1 = non privilegiato (il prompt è `router>`), il livello predefinito per l'accesso
- livello di privilegio 15 = privilegiato (il prompt è `router#`), il livello dopo l'attivazione della modalità di abilitazione
- livello di privilegio 0 = utilizzato raramente, ma include 5 comandi: **disabilita**, **abilita**, **esci**, **guida** e **disconnetti**

I livelli da 2 a 14 non vengono utilizzati in una configurazione predefinita, ma i comandi che normalmente si trovano al livello 15 possono essere spostati verso il basso fino a uno di questi livelli e i comandi che normalmente si trovano al livello 1 possono essere spostati verso l'alto fino a uno di questi livelli. Ovviamente, questo modello di sicurezza implica alcune attività di amministrazione sul router.

Per determinare il livello di privilegio come utente connesso, digitare il comando **show privilege**. Per determinare i comandi disponibili con un determinato livello di privilegio per la versione del

software Cisco IOS® in uso, digitare **?** dalla riga di comando quando si esegue l'accesso a tale livello di privilegio.

Nota: anziché assegnare livelli di privilegio, è possibile eseguire l'autorizzazione dei comandi se il server di autenticazione supporta TACACS+. Il protocollo RADIUS non supporta l'autorizzazione dei comandi.

Componenti usati

Per questo documento, è stato usato il software Cisco IOS versione 11.2 e successive.

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.

Esempio

In questo esempio, i comandi **snmp-server** vengono spostati dal livello di privilegio 15 (predefinito) al livello di privilegio 7. Il comando **ping** viene spostato dal livello di privilegio 1 al livello di privilegio 7. Quando l'utente 7 viene autenticato, il server assegna a tale utente il livello di privilegio 7 e il comando **show privilege** visualizza "Il livello di privilegio corrente è 7." L'utente può eseguire il ping e la configurazione del server snmp in modalità di configurazione. Altri comandi di configurazione non sono disponibili.

Configurazioni - Router

Router - 11.2

```
aaa new-model
aaa authentication login default tacacs+|radius local
aaa authorization exec tacacs+|radius local
username backup privilege 7 password 0 backup
tacacs-server host 171.68.118.101
tacacs-server key cisco
radius-server host 171.68.118.101
radius-server key cisco
privilege configure level 7 snmp-server host
privilege configure level 7 snmp-server enable
privilege configure level 7 snmp-server
privilege exec level 7 ping
privilege exec level 7 configure terminal
privilege exec level 7 configure
```

Router - 11.3.3.T e versioni successive (fino a 12.0.5.T)

```
aaa new-model
aaa authentication login default tacacs+|radius local
aaa authorization exec default tacacs+|radius local
username backup privilege 7 password 0 backup
tacacs-server host 171.68.118.101
tacacs-server key cisco
radius-server host 171.68.118.101
radius-server key cisco
privilege configure level 7 snmp-server host
privilege configure level 7 snmp-server enable
privilege configure level 7 snmp-server
privilege exec level 7 ping
privilege exec level 7 configure terminal
privilege exec level 7 configure
```

Router - 12.0.5.T e versioni successive

```
aaa new-model
aaa authentication login default group tacacs+|radius local
aaa authorization exec default group tacacs+|radius local
username backup privilege 7 password 0 backup
tacacs-server host 171.68.118.101
tacacs-server key cisco
radius-server host 171.68.118.101
radius-server key cisco
privilege configure level 7 snmp-server host
privilege configure level 7 snmp-server enable
privilege configure level 7 snmp-server
privilege exec level 7 ping
privilege exec level 7 configure terminal
privilege exec level 7 configure
```

Configurazioni - Server

Cisco Secure NT TACACS+

Attenersi alla procedura seguente per configurare il server.

1. Immettere il nome utente e la password.
2. In Impostazioni gruppo verificare che shell/exec sia selezionato e che 7 sia stato immesso nella casella del livello di privilegio.

TACACS+ - Stanza in Freeware Server

```
Stanza in TACACS+ freeware:
user = seven {
login = cleartext seven
service = exec {
priv-lvl = 7
}
}
```

Cisco Secure UNIX TACACS+

```
user = seven {
password = clear "seven"
service = shell {
```

```
set priv-lvl = 7
}
}
```

Cisco Secure NT RADIUS

Attenersi alla procedura seguente per configurare il server.

1. Immettere il nome utente e la password.
2. In Group Settings for IETF, Service-type (attributo 6) = **Nas-Prompt**
3. Nell'area CiscoRADIUS, selezionare **AV-Pair**, quindi nella casella rettangolare sottostante immettere **shell:priv-lvl=7**.

Cisco Secure UNIX RADIUS

```
user = seven{
radius=Cisco {
check_items= {
2="seven"
}
reply_attributes= {
6=7
9,1="shell:priv-lvl=7"
}
}
}
```

Questo è il file utente per il nome utente "sette".

Nota: il server deve supportare coppie di cavi av Cisco.

- sette password = **passwdxyz**
- Service-Type = **Shell-User**
- cisco-avpair =**shell:priv-lvl=7**

Informazioni correlate

- Pagina di supporto RADIUS
- RFC (Requests for Comments)
- Documentazione relativa a TACACS+ in IOS
- Pagina di supporto TACACS+
- Pagina di supporto per Cisco Secure UNIX
- Pagina di supporto di Cisco Secure ACS per Windows
- Supporto tecnico – Cisco Systems