Risoluzione dei problemi relativi a CSS e TACACS+

Sommario

Introduzione

Il protocollo TACACS+ (Terminal Access Controller Access Control System) fornisce il controllo dell'accesso per router, server di accesso alla rete (NAS) o altri dispositivi tramite uno o più server daemon. Esegue la crittografia di tutto il traffico tra NAS e daemon utilizzando le comunicazioni TCP per una consegna affidabile.

In questo documento vengono fornite informazioni sulla risoluzione dei problemi per i software Content Services Switch (CSS) e TACACS+. È possibile configurare il CSS come client di un server TACACS+, fornendo un metodo per l'autenticazione degli utenti e l'autorizzazione e l'accounting dei comandi di configurazione e non di configurazione. Questa funzionalità è disponibile in WebNS 5.03.

Nota: per ulteriori informazioni, fare riferimento a Configurazione del CSS come client di un server TACACS+.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

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

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.

Problema

Quando si tenta di accedere a CSS con un utente TACACS+, l'accesso non funziona.

Comandi Solution e debug

In genere, quando l'autenticazione TACACS+ non funziona con un foglio di stile CSS, il problema è in genere dovuto a un problema di configurazione sul server CSS o TACACS+. È innanzitutto necessario verificare se il file CSS è stato configurato come client di un server TACACS+.

Dopo aver selezionato questa opzione, è possibile utilizzare ulteriori funzioni di registrazione sul foglio di stile CSS per determinare il problema. Completare questa procedura per attivare la registrazione.

In CSS, accedere alla modalità di debug.

```
CSS# llama
CSS(debug)# mask tac 0x3
CSS(debug)# exit
CSS# configure
CSS(config)# logging subsystem security level debug-7
CSS(config)# logging subsystem netman level info-6
CSS(config)# exit
CSS# logon
!--- This logs messages to the screen.
```

Per disabilitare la registrazione, usare questi comandi:

```
CSS# llama
CSS(debug)# mask tac 0x0
CSS(debug)# exit
CSS# no logon
```

Possono essere visualizzati i seguenti messaggi:

```
SEP 10 08:30:10 5/1 99 SECURITY-7: SECMGR:SecurityAuth:Request from 0x20204b0c
SEP 10 08:30:10 5/1 100 SECURITY-7: SECMGR:SecurityMgrProc:Try Primary
SEP 10 08:30:10 5/1 101 SECURITY-7: Security Manager sending error 7 reply to
ller 20201c00
```

Questi messaggi indicano che il CSS tenta di comunicare con il server TACACS+, ma che il server TACACS+ rifiuta il CSS. L'`errore 7` indica che la chiave TACACS+ immessa nel CSS non

corrisponde alla chiave sul server TACACS+.

Se l'accesso tramite un server TACACS+ ha esito positivo, viene visualizzato questo messaggio (notare la risposta `0` di invio `riuscita`):

```
SEP 10 08:31:46 5/1 107 SECURITY-7: SECMGR:SecurityAuth:Request from 0x20204b0d
SEP 10 08:31:46 5/1 108 SECURITY-7: SECMGR:SecurityMgrProc:Try Primary
SEP 10 08:31:47 5/1 109 SECURITY-7: Security Manager sending success 0 reply to
caller 20201c00

SEP 10 08:31:47 5/1 110 SECURITY-7: SECMGR:SecurityMgrProc:Try Done, Send 0x2020
4b0d
```

Errori comuni

L'errore più comune quando si imposta un foglio di stile CSS per lavorare con un server TACACS+ è in realtà molto semplice. Questo comando indica al CSS il tasto da utilizzare per comunicare con il server TACACS+:

```
CSS(config)# tacacs-server key system enterkeyhere
```

La chiave può essere in testo non crittografato o crittografata con DES. La chiave non crittografata viene crittografata da DES prima di essere inserita nella configurazione in esecuzione. Per rendere chiaro un testo chiave, racchiuderlo tra virgolette. Per crittografare DES, non utilizzare virgolette. È importante sapere se la chiave TACACS+ è crittografata con DES o se la chiave è in formato testo non crittografato. Dopo aver eseguito il comando, far corrispondere la chiave del foglio di stile CSS alla chiave utilizzata dal server TACACS+.

Informazioni correlate

- Configurazione di CSS come client di un server TACACS+
- Configurazione di TACACS+ ed Extended TACACS+
- Documentazione e supporto tecnico – Cisco Systems