Problemi di autenticazione RADIUS in ONS 15454 versione 6.0

Sommario

Introduzione

Questo documento descrive un paio di problemi noti relativi all'autenticazione server RADIUS (Remote Authentication Dial-In User Service) in ONS 15454 versione 6.0 in un ambiente Cisco ONS 15454.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco ONS 15454
- server RADIUS

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco ONS 15454 versione 6.0

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.

Premesse

RADIUS 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 dai tre componenti seguenti:

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

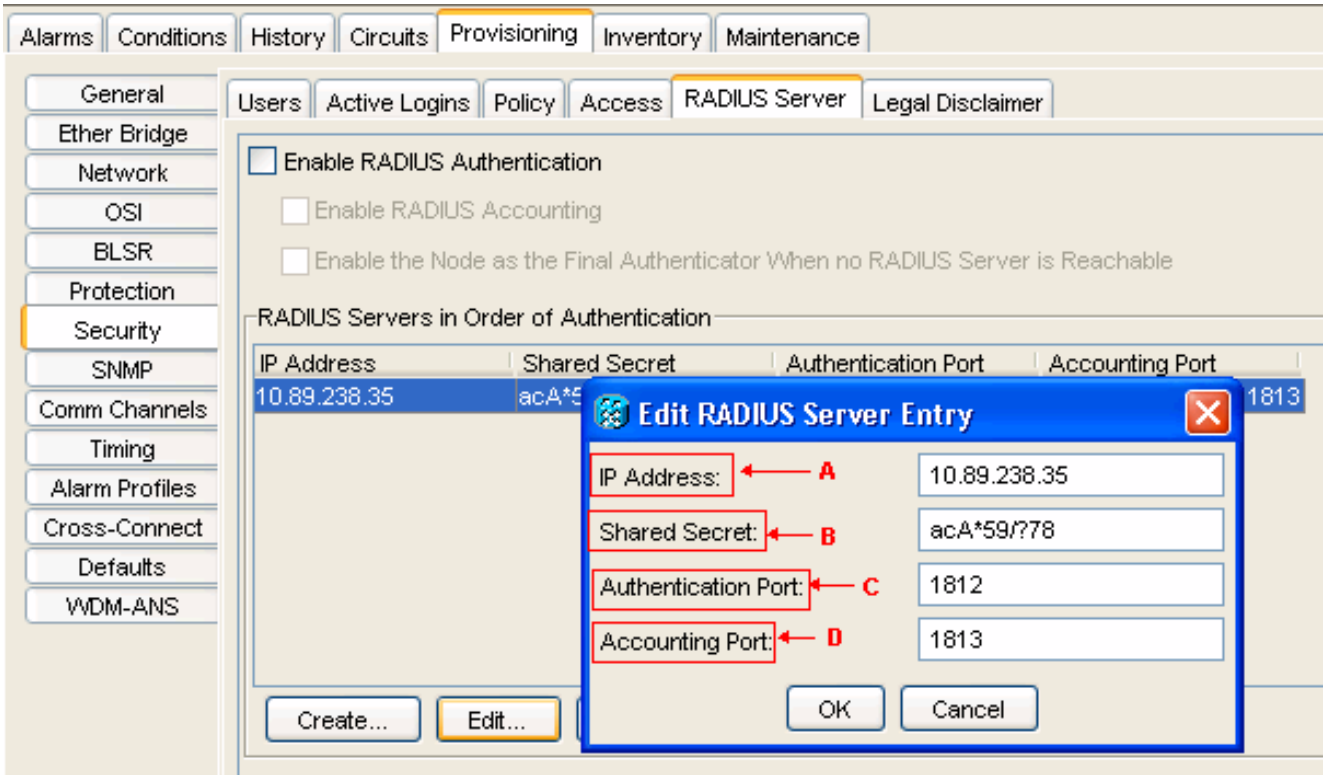
Un nodo ONS 15454 funziona come client di RADIUS. Il client passa le informazioni utente ai server RADIUS designati e quindi agisce sulla risposta. I server RADIUS ricevono le richieste di connessione degli utenti, autenticano l'utente e restituiscono tutte le informazioni di configurazione necessarie al client per fornire il servizio all'utente.

Un segreto condiviso autentica le transazioni tra il client RADIUS e il server. Il segreto condiviso non viene mai inviato tramite la rete. Inoltre, tutte le password utente vengono crittografate quando vengono scambiate tra il client e il server RADIUS. Il processo di crittografia elimina la possibilità che un utente esegua il monitoraggio di una rete non protetta per determinare la password di un utente.

Segreto condiviso

Un segreto condiviso è una stringa di testo che funge da password tra il client RADIUS ONS15454 e il server RADIUS. Completare questi passaggi per creare un segreto condiviso:

1. Accedere a Cisco Transport Controller (CTC).
2. Passare alla visualizzazione Rete.
3. Selezionare uno specifico ONS 15454 per passare alla visualizzazione scaffale.
4. Fare clic su **Provisioning > Security > RADIUS Server**.
5. Digitare l'indirizzo IP del server RADIUS nel campo Indirizzo IP (vedere la freccia A nella Figura 1).
6. Digitare un segreto condiviso nel campo Segreto condiviso. Un segreto condiviso è una stringa di testo che funge da password tra un client RADIUS e un server RADIUS (vedere la freccia B nella Figura 1).
7. Digitare il numero della porta di autenticazione RADIUS nel campo Porta di autenticazione (vedere la freccia C nella Figura 1).Il numero della porta di autenticazione predefinita è 1812. Se il nodo è un ENE, impostare la porta di autenticazione su un numero compreso tra 1860 e 1869.
8. Digitare il numero della porta di accounting RADIUS nel campo Porta di accounting (vedere la freccia D nella Figura 1).Il numero di porta di accounting predefinito è 1813. Se il nodo è un ENE, impostare la porta di accounting su un numero compreso tra 1870 e 1879.**Figura 1 - Sicurezza: Server RADIUS**



Utilizzare i segreti condivisi per assicurarsi che un dispositivo abilitato per RADIUS configurato con lo stesso segreto condiviso invii tutti i messaggi RADIUS ad eccezione del messaggio Access-Request.

I segreti condivisi garantiscono che il messaggio RADIUS non venga modificato durante la trasmissione. In altre parole, i segreti condivisi mantengono l'integrità dei messaggi. I segreti condivisi consentono inoltre di crittografare alcuni attributi RADIUS, ad esempio User-Password e Tunnel-Password.

ONS 15454 versione 6.0 limita la lunghezza di un segreto condiviso a 16 caratteri. Tuttavia, a partire da ONS 15454 versione 6.2, Cisco prevede di aumentare la lunghezza massima a 128 caratteri. per ulteriori informazioni, fare riferimento all'ID bug Cisco CSCsc16614 (solo utenti registrati).

Il gruppo di caratteri segreti condivisi supporta:

- Lettere (maiuscole e minuscole), ad esempio A, B, a e b.
- Numeri, ad esempio 1, 2 e 3.
- Simboli che rappresentano tutti i caratteri non definiti come lettere o numeri, ad esempio >, (e *.

Mapping gruppi di sicurezza utenti

Una coppia attributo-valore (AV) rappresenta una variabile e uno dei possibili valori che la variabile può contenere. In ONS 15454, gli utenti sono mappati su diversi gruppi di sicurezza basati su Cisco AV Pair. Di seguito è riportato un esempio:

"shell:priv-lvl=X" dove X può avere un valore compreso tra 0 e 3:

- 0 rappresenta RTRV.
- 1 rappresenta PROV.

- 2 rappresenta MAINT.
- 3 rappresenta SUPER.

Password

Il server e il client RADIUS non limitano i caratteri utilizzati per una password. Tuttavia, la CTC ha un limite. Per ONS 15454 versione 6.0, di seguito sono riportati i caratteri supportati da CTC:

- Lettere (maiuscole e minuscole), ad esempio A, B, a e b.
- Numeri, ad esempio 1, 2 e 3.
- Solo i simboli speciali #, % e +.

Cisco intende rimuovere la limitazione relativa ai simboli speciali nelle versioni più recenti di ONS 15454. Per ulteriori informazioni, fare riferimento all'ID bug Cisco CSCsc16604 (solo utenti registrati).

Informazioni correlate

- Documentazione e supporto tecnico – Cisco Systems