Verifica della connettività del server Radius con il comando Test AAA Radius

Sommario

Introduzione

In questo documento viene descritto come usare il comando **test aaa radius** sul WLC Cisco per identificare i problemi di connettività del server radius e di autenticazione del client senza usare un client wireless.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza del codice 8.2 e superiore del controller WLC (Wireless LAN Controller).

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.

Premesse

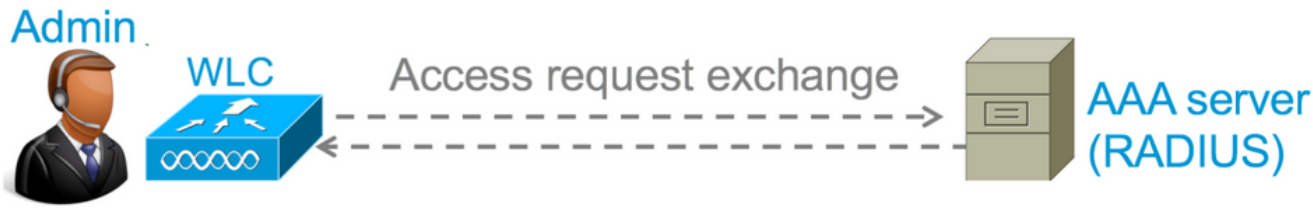
I problemi di autenticazione dei client wireless sono uno dei più difficili problemi che i tecnici delle reti wireless devono affrontare. Per risolvere il problema, spesso è necessario entrare in possesso

del client problematico, lavorare con gli utenti finali che non possono avere la migliore conoscenza delle reti wireless e raccogliere debug e acquisizioni. In una rete wireless sempre più importante, questo può causare tempi di inattività significativi.

Finora non era possibile identificare facilmente se un errore di autenticazione era causato dal server RADIUS che rifiuta il client o semplicemente da un problema di raggiungibilità. Il comando **test aaa radius** consente di eseguire questa operazione. È ora possibile verificare in remoto se la comunicazione del server WLC-Radius non riesce o se le credenziali del client determinano un'autenticazione riuscita o non riuscita.

Funzionamento Della Funzionalità

Si tratta di un flusso di lavoro di base quando si utilizza il comando **test aaa radius**, come mostrato nell'immagine.



Passaggio 1. Il WLC invia un messaggio di richiesta di accesso al server radius insieme ai parametri menzionati nel comando **test aaa radius**.

Ad esempio: **test aaa radius username admin password cisco123 wlan-id 1 apgroup default-group server-index 2**

Passaggio 2. Il server RADIUS convalida le credenziali fornite e fornisce i risultati della richiesta di autenticazione.

Sintassi dei comandi

Per eseguire il comando è necessario specificare i seguenti parametri:

(Cisco Controller) > **test aaa radius nomeutente <nome utente> password <password> id-wlan <id-wlan> apgroup <nome-gruppo-apgroup> indice-server <indice-server>**

```
<username>                    ---> Username that you are testing.
<password>                    ---> Password that you are testing
<wlan-id>                     ---> WLAN ID of the SSID that you are testing.
<apgroup-name>  (optional)    ---> AP group name. This will be default-group if there is no AP
group configured.
<server-index>      (optional)  ---> The server index configured for the radius server that you
are trying to test. This can be found under Security > Authentication tab.
```

Scenario 1. Tentativo di autenticazione superato

Esaminiamo più in dettaglio il funzionamento del comando e gli output vengono visualizzati

quando il comando **test aaa radius** restituisce un'autenticazione riuscita. Quando il comando viene eseguito, WLC visualizza i parametri con cui invia la richiesta di accesso:

```
(Cisco Controller) >test aaa radius username admin password cisco123 wlan-id 1 apgroup default-
group server-index 2
Radius Test Request
  Wlan-id..................................... 1
  ApGroup Name................................ default-group
  Attributes                    Values
  ----------                    ------
  User-Name                     admin
  Called-Station-Id             00:00:00:00:00:00:WLC5508
  Calling-Station-Id            00:11:22:33:44:55
  Nas-Port                      0x0000000d (13)
  Nas-Ip-Address                10.20.227.39
  NAS-Identifier                WLC_5508
  Airespace / WLAN-Identifier   0x00000001 (1)
  User-Password                 cisco123
  Service-Type                  0x00000008 (8)
  Framed-MTU                    0x00000514 (1300)
  Nas-Port-Type                 0x00000013 (19)
  Tunnel-Type                   0x0000000d (13)
  Tunnel-Medium-Type            0x00000006 (6)
  Tunnel-Group-Id               0x00000051 (81)
  Cisco / Audit-Session-Id      ad14e327000000c466191e23
  Acct-Session-Id               56131b33/00:11:22:33:44:55/210
test radius auth request successfully sent. Execute 'test aaa show radius' for response
```

Per visualizzare i risultati della richiesta di autenticazione, è necessario eseguire il comando **test aaa show radius**. La visualizzazione dell'output del comando può richiedere del tempo se un server radius non è raggiungibile e il WLC deve riprovare o eseguire il fallback su un server radius diverso.

```
(Cisco Controller) >test aaa show radius
Radius Test Request
  Wlan-id..................................... 1
  ApGroup Name................................ default-group
  Server Index................................ 2
Radius Test Response
Radius Server         Retry Status
-------------         ----- ------
10.20.227.52            1   Success
Authentication Response:
  Result Code: Success
  Attributes                    Values
  ----------                    ------
  User-Name                     admin
  Class                         CACS:rs-acs5-6-0-22/230677882/20313
  Session-Timeout               0x0000001e (30)
  Termination-Action            0x00000000 (0)
  Tunnel-Type                   0x0000000d (13)
  Tunnel-Medium-Type            0x00000006 (6)
  Tunnel-Group-Id               0x00000051 (81)
```

L'aspetto estremamente utile di questo comando è la visualizzazione degli attributi restituiti dal server radius. Può essere un URL di reindirizzamento o un ACL (Access Control List). Ad esempio, in caso di autenticazione Web centrale (CWA) o di informazioni VLAN quando si usa l'override della VLAN.

Attenzione: Il nome utente e la password nella richiesta di accesso vengono inviati in formato testo non crittografato al server radius, quindi è necessario utilizzarli con cautela se il traffico passa attraverso una rete non protetta.

Scenario 2: Tentativo di autenticazione non riuscito

L'output viene visualizzato quando una voce di nome utente/password genera un errore di autenticazione.

```
(Cisco Controller) >test aaa show radius
Radius Test Request
  Wlan-id..................................... 1
  ApGroup Name................................ default-group
  Server Index................................ 2
Radius Test Response
Radius Server            Retry Status
-------------            ----- ------
10.20.227.52            1     Success
Authentication Response:
  Result Code: Authentication failed  ------>This indicates that the user authentication will
fail.
  No AVPs in Response
```

In questo caso, il test di connettività ha avuto esito positivo, tuttavia il server RADIUS ha inviato un messaggio di rifiuto di accesso per la combinazione di nome utente e password utilizzata.

Scenario 3: Comunicazione non riuscita tra WLC e server Radius

```
(Cisco Controller) >test aaa show radius
 previous test command still not completed, try after some time
```

Prima di visualizzare l'output, è necessario attendere il completamento dei tentativi del WLC. La durata può variare in base alle soglie configurate per i nuovi tentativi.

```
(Cisco Controller) >test aaa show radius
Radius Test Request
  Wlan-id..................................... 1
  ApGroup Name................................ default-group
  Server Index................................ 3
Radius Test Response
Radius Server            Retry Status
-------------            ----- ------
10.20.227.72            6     No response received from server
Authentication Response:
  Result Code: No response received from server
  No AVPs in Response
```

In questo output si nota che il WLC ha tentato di contattare il server radius per 6 volte e, in assenza di risposta, il server radius è stato contrassegnato come non raggiungibile.

Scenario 4: Radius Fallback

Quando sono configurati più server RADIUS con l'SSID (Service Set Identifier) e il server RADIUS primario non risponde, il WLC tenta di utilizzare il server RADIUS secondario configurato. Questo viene mostrato in modo molto chiaro nell'output in cui il primo server radius non risponde e il WLC prova quindi con il secondo server radius che risponde immediatamente.

```
(Cisco Controller) >test aaa show radius
Radius Test Request
  Wlan-id..................................... 1
  ApGroup Name................................ default-group
Radius Test Response
Radius Server            Retry Status
-------------            ----- ------
10.20.227.62            6     No response received from server
10.20.227.52            1     Success
Authentication Response:
  Result Code: Success
  Attributes                    Values
  ----------                    ------
  User-Name                     admin
```

Avvertenze

- Attualmente non è disponibile il supporto GUI. È solo un comando che può essere eseguito dal WLC.
- La verifica riguarda solo il raggio. Non può essere utilizzato per l'autenticazione TACACS.
- Impossibile testare l'autenticazione locale di Flexconnect con questo metodo.

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).