Autenticazione dell'amministratore della sala di attesa del controller LAN wireless tramite server RADIUS

Sommario

Introduzione

In questo documento viene descritta la procedura di configurazione necessaria per autenticare un amministratore della sala di attesa del controller WLC (Wireless LAN Controller) con un server RADIUS.

Prerequisiti

Requisiti

Prima di provare questa configurazione, accertarsi di soddisfare i seguenti requisiti:

- Informazioni su come configurare i parametri di base sui WLC
- Informazioni su come configurare un server RADIUS, ad esempio Cisco Secure ACS
- Conoscenza degli utenti guest nel WLC

Componenti usati

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

hardware:

- Cisco Wireless LAN Controller 4400 con versione 7.0.216.0
- Cisco Secure ACS con software versione 4.1 e utilizzato come server RADIUS in questa configurazione.

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

Un amministratore della sala di attesa, noto anche come ambasciatore della sala di attesa di un WLC, può creare e gestire account utente guest sul controller WLC (Wireless LAN Controller). L'ambasciatore della sala di attesa dispone di privilegi di configurazione limitati e può accedere solo alle pagine Web utilizzate per gestire gli account guest. L'ambasciatore della sala di attesa può specificare il periodo di tempo durante il quale gli account utente guest rimangono attivi. Trascorso il tempo specificato, gli account utente guest scadono automaticamente.

Per ulteriori informazioni sugli utenti guest, consultare la Guida all'implementazione: Cisco Guest Access Using the Cisco Wireless LAN Controller.

Per creare un account utente guest sul WLC, è necessario accedere al controller come amministratore della sala di attesa. Questo documento spiega come un utente viene autenticato nel WLC come amministratore di sala di attesa in base agli attributi restituiti dal server RADIUS.

Nota: l'autenticazione dell'amministratore della sala di attesa può essere eseguita anche in base all'account dell'amministratore della sala di attesa configurato localmente sul WLC. Per informazioni su come creare localmente un account di amministratore della sala d'attesa su un controller, fare riferimento a Creazione di un account di amministratore della sala d'attesa.

Configurazione

In questa sezione vengono presentate le informazioni su come configurare il WLC e i Cisco Secure ACS per lo scopo descritto in questo documento.

Configurazioni

In questo documento vengono usate le seguenti configurazioni:

- L'indirizzo IP dell'interfaccia di gestione del WLC è 10.77.244.212/27.
- L'indirizzo IP del server RADIUS è 10.77.244.197/27.
- La chiave segreta condivisa utilizzata sul punto di accesso e sul server RADIUS è cisco123.
- Il nome utente e la password dell'amministratore della sala di attesa configurato nel server RADIUS sono entrambi lobbyadmin.

Nell'esempio di configurazione illustrato in questo documento, a qualsiasi utente che accede al controller con nome utente e password di lobbyadmin viene assegnato il ruolo di amministratore di lobby.

Configurazione WLC

Prima di avviare la configurazione WLC necessaria, verificare che sul controller sia in esecuzione la versione 4.0.206.0 o successive. Ciò è dovuto all'ID bug Cisco CSCsg89868 (solo utenti registrati) sul quale l'interfaccia Web del controller visualizza pagine Web errate per l'utente LobbyAdmin quando il nome utente è archiviato in un database RADIUS. L'interfaccia LobbyAdmin viene presentata con l'interfaccia ReadOnly invece che con l'interfaccia LobbyAdmin.

Il bug è stato risolto nella versione WLC 4.0.206.0. Pertanto, verificare che la versione del controller sia 4.0.206.0 o successiva. Per istruzioni su come aggiornare il controller alla versione appropriata, fare riferimento al documento sull'aggiornamento del software Wireless LAN Controller (WLC).

Per eseguire l'autenticazione di gestione del controller con il server RADIUS, verificare che il flag Admin-auth-via-RADIUS sia abilitato sul controller. È possibile verificare questa condizione dall'output del comando show radius summary.

Il primo passaggio consiste nel configurare le informazioni del server RADIUS sul controller e stabilire la raggiungibilità di livello 3 tra il controller e il server RADIUS.

Configurare le informazioni del server RADIUS sul controller

Completare questa procedura per configurare il WLC con i dettagli sull'ACS:

1. Dall'interfaccia utente del WLC, scegliere la scheda Security e configurare l'indirizzo IP e il segreto condiviso del server ACS.

   Affinché il WLC possa comunicare con l'ACS, questo segreto condiviso deve essere lo stesso sull'ACS.

   Nota: il segreto condiviso ACS fa distinzione tra maiuscole e minuscole. Pertanto, assicurarsi di immettere correttamente le informazioni segrete condivise.

   Nella figura viene illustrato un esempio:

2. Selezionare la casella di controllo Management (Gestione) per consentire all'ACS di gestire

gli utenti WLC, come mostrato nella figura del passaggio 1. Quindi, fare clic su Apply (Applica).

3. Verificare la raggiungibilità di layer 3 tra il controller e il server RADIUS configurato con l'ausilio del comando ping. Questa opzione ping è disponibile anche nella pagina del server RADIUS configurato nell'interfaccia utente del WLC della scheda Sicurezza>Autenticazione RADIUS.

   Nel diagramma viene mostrata una risposta ping dal server RADIUS riuscita. Pertanto, tra il controller e il server RADIUS è disponibile la raggiungibilità di layer 3.

Configurazione server RADIUS

Per configurare il server RADIUS, completare la procedura descritta nelle sezioni seguenti:

1. Aggiungere il WLC come client AAA al server RADIUS
2. Configurare l'attributo del tipo di servizio IETF RADIUS appropriato per un amministratore di sala d'attesa

Aggiungere il WLC come client AAA al server RADIUS

Completare questa procedura per aggiungere il WLC come client AAA nel server RADIUS. Come accennato in precedenza, in questo documento viene utilizzato ACS come server RADIUS. Per questa configurazione è possibile utilizzare qualsiasi server RADIUS.

Completare questi passaggi per aggiungere il WLC come client AAA nell'ACS:

1. Dall'interfaccia utente di ACS, selezionare la scheda Network Configuration (Configurazione di rete).
2. In Client AAA, fare clic su Add Entry (Aggiungi voce).
3. Nella finestra Add AAA Client, immettere il nome host del WLC, l'indirizzo IP del WLC e una chiave segreta condivisa. Vedere l'esempio di diagramma al punto 5.
4. Dal menu a discesa Autentica tramite, scegliere RADIUS (Cisco Aironet).
5. Per salvare la configurazione, fare clic su Submit + Restart (Invia + Riavvia).

Configurare l'attributo del tipo di servizio IETF RADIUS appropriato per un amministratore di sala d'attesa

Per autenticare un utente di gestione di un controller come amministratore della sala di attesa tramite il server RADIUS, è necessario aggiungere l'utente al database RADIUS con l'attributo IETF RADIUS Service-Type impostato su Callback Administrative. Questo attributo assegna all'utente specifico il ruolo di amministratore della sala di attesa in un controller.

In questo documento viene illustrato l'esempio dell'utente lobbyadmin come amministratore di

lobby. Per configurare l'utente, eseguire la procedura seguente sul server ACS:

1. Dalla GUI di ACS, selezionare la scheda User Setup (Configurazione utente).
2. Immettere il nome utente da aggiungere ad ACS come mostrato nella finestra di esempio:
3. Fare clic su Add/Edit (Aggiungi/Modifica) per accedere alla pagina User Edit (Modifica utente).
4. Nella pagina Modifica utente specificare il nome reale, la descrizione e la password dell'utente.

   In questo esempio, il nome utente e la password utilizzati sono entrambi lobbyadmin.
5. Scorrere verso il basso fino all'impostazione Attributi RADIUS IETF e selezionare la casella di controllo Attributo tipo di servizio.
6. Scegliere Callback Administrative dal menu a discesa Service-Type e fare clic su Submit.

   Attributo che assegna all'utente il ruolo di amministratore di sala di attesa.

   A volte questo attributo Service-Type non è visibile nelle impostazioni utente. In questi casi, completare la procedura seguente per renderla visibile:

   a. Dalla GUI di ACS, selezionare Interface Configuration > RADIUS (IETF) per abilitare gli attributi IETF nella finestra User Configuration.

      Viene visualizzata la pagina Impostazioni RADIUS (IETF).

   b. Nella pagina Impostazioni RADIUS (IETF) è possibile attivare l'attributo IETF che deve essere visibile in Impostazioni utente o gruppo. Per questa configurazione, selezionare Service-Type per la colonna User e fare clic su Submit.

      In questa finestra viene visualizzato un esempio:

      Nota: in questo esempio viene specificata l'autenticazione per singolo utente. È inoltre possibile eseguire l'autenticazione in base al gruppo a cui appartiene un determinato utente. In questi casi, selezionare la casella di controllo Raggruppa in modo che l'attributo sia visibile in Impostazioni gruppo.

      Nota: inoltre, se l'autenticazione avviene su base di gruppo, è necessario assegnare gli utenti a un determinato gruppo e configurare gli attributi IETF dell'impostazione di gruppo in modo da fornire i privilegi di accesso agli utenti di tale gruppo. Per informazioni dettagliate su come configurare e gestire i gruppi, fare riferimento a Gestione gruppi utenti.

Verifica

Fare riferimento a questa sezione per verificare che la configurazione funzioni correttamente.

Per verificare che la configurazione funzioni correttamente, accedere al WLC tramite la modalità GUI (HTTP/HTTPS).

Nota: un ambasciatore della sala di attesa non può accedere all'interfaccia CLI del controller e può quindi creare account utente guest solo dalla GUI del controller.

Quando viene visualizzato il prompt di accesso, immettere il nome utente e la password configurati nell'ACS. Se le configurazioni sono corrette, l'autenticazione nel WLC come amministratore della sala di attesa è riuscita. Nell'esempio viene mostrato come la GUI di un amministratore di sala di attesa viene visualizzata dopo la riuscita dell'autenticazione:

Nota: è possibile notare che l'amministratore della sala di attesa non dispone di altre opzioni oltre alla gestione degli utenti guest.

Per verificarlo dalla modalità CLI, accedere al controller in modalità Telnet come amministratore di lettura/scrittura. Eseguire il comando debug aaa all enable dalla CLI del controller.

```
<#root>

(Cisco Controller) >

debug aaa all enable


(Cisco Controller) >
*aaaQueueReader: Aug 26 18:07:35.072: ReProcessAuthentication previous proto 28,
 next proto 20001
*aaaQueueReader: Aug 26 18:07:35.072: AuthenticationRequest: 0x3081f7dc
*aaaQueueReader: Aug 26 18:07:35.072:   Callback.....................................0x10756dd0
*aaaQueueReader: Aug 26 18:07:35.072:   protocolType.................................0x00020001
*aaaQueueReader: Aug 26 18:07:35.072:   proxyState....................................00:00:00:40:
00:00-00:00
*aaaQueueReader: Aug 26 18:07:35.072:   Packet contains 5 AVPs (not shown)
*aaaQueueReader: Aug 26 18:07:35.072: apfVapRadiusInfoGet: WLAN(0) dynamic int attributes srcAddr:
0x0, gw:0x0, mask:0x0, vlan:0, dpPort:0, srcPort:0
*aaaQueueReader: Aug 26 18:07:35.073: 00:00:00:40:00:00 Successful transmission of Authentication
Packet (id 39) to 10.77.244.212:1812, proxy state 00:00:00:40:00:00-00:01
*aaaQueueReader: Aug 26 18:07:35.073: 00000000: 01 27 00 47 00 00 00 00  00 00 00 00 00 00 00 00
.'.G............
*aaaQueueReader: Aug 26 18:07:35.073: 00000010: 00 00 00 00 01 0c 6c 6f  62 62 79 61 64 6d 69 6e
......lobbyadmin
*aaaQueueReader: Aug 26 18:07:35.073: 00000020: 02 12 5f 5b 5c 12 c5 c8  52 d3 3f 4f 4f 8e 9d 38
 .._[\...R.?OO..8
*aaaQueueReader: Aug 26 18:07:35.073: 00000030: 42 91 06 06 00 00 00 07  04 06 0a 4e b1 1a 20 09
B..........N....
*aaaQueueReader: Aug 26 18:07:35.073: 00000040: 57 4c 43 34 34 30 30 WLC4400
*radiusTransportThread: Aug 26 18:07:35.080: 00000000: 02 27 00 40 7e 04 6d 533d ed 79 9c b6 99 d1
f8  .'.@~.mS=.y.....
*radiusTransportThread: Aug 26 18:07:35.080: 00000010: d0 5a 8f 4f 08 06 ff ffff ff 06 06 00 00 00
0b  .Z.O............
*radiusTransportThread: Aug 26 18:07:35.080: 00000020: 19 20 43 41 43 53 3a 302f 61 65 32 36 2f 61
34  ..CACS:0/ae26/a4
*radiusTransportThread: Aug 26 18:07:35.080: 00000030: 65 62 31 31 61 2f 6c 6f62 62 79 61 64 6d 69
6e  eb11a/lobbyadmin
*radiusTransportThread: Aug 26 18:07:35.080: ****Enter processIncomingMessages: response code=2
*radiusTransportThread: Aug 26 18:07:35.080: ****Enter processRadiusResponse: response code=2
*radiusTransportThread: Aug 26 18:07:35.080: 00:00:00:40:00:00 Access-Accept received from RADIUS
```

```
server 10.77.244.212 for mobile 00:00:00:40:00:00 receiveId = 0
*radiusTransportThread: Aug 26 18:07:35.080: AuthorizationResponse: 0x13c73d50
*radiusTransportThread: Aug 26 18:07:35.080:    structureSize.............................118
*radiusTransportThread: Aug 26 18:07:35.080:    resultCode................................0
*radiusTransportThread: Aug 26 18:07:35.080:    protocolUsed..............................0x00000001
*radiusTransportThread: Aug 26 18:07:35.080:    proxyState................................00:00:00:4
*radiusTransportThread: Aug 26 18:07:35.080:    Packet contains 3 AVPs:
*radiusTransportThread: Aug 26 18:07:35.080:        AVP[01] Framed-IP-Address.....................0x
*radiusTransportThread: Aug 26 18:07:35.080:
```

AVP[02] Service-Type.....0x0000000b (11) (4 bytes

)
*radiusTransportThread: Aug 26 18:07:35.080:

AVP[03] Class.....
CACS:0/ae26/a4eb11a/lobbyadmin (30 bytes)

***emWeb: Aug 26 18:07:35.084: Authentication succeeded for lobbyadmin**

Nelle informazioni evidenziate in questo output, è possibile notare che l'attributo del tipo di servizio 11 (Callback Administrative) viene passato al controller dal server ACS e che l'utente ha eseguito l'accesso come amministratore della sala di attesa.

Questi comandi possono essere di aiuto aggiuntivo:

- abilitazione dettagli debug aaa
- debug aaa events enable
- abilitazione pacchetti debug aaa

Nota: fare riferimento a Informazioni importanti sui comandi di debug prima di usare i comandi debug.

Risoluzione dei problemi

Quando si accede a un controller con privilegi di ambasciatore di sala di attesa, non è possibile creare un account utente guest con un valore di durata pari a "0", ovvero un account che non scade mai. In questi casi, viene visualizzato il messaggio di errore `Lifetime value cannot be 0 (La durata non può essere 0).`

Ciò è dovuto all'ID bug Cisco CSCsf32392 (solo utenti registrati), riscontrato principalmente nella versione 4.0 del WLC. Il bug è stato risolto nella versione WLC 4.1.

Informazioni correlate

- Esempio di autenticazione server RADIUS di utenti di gestione sulla configurazione del controller
- Configurazione Cisco Unified Wireless Network TACACS+
- Guida alla configurazione di Cisco Wireless LAN Controller, versione 4.0 - Gestione degli

account utente
- Esempio di configurazione di ACL sui Wireless LAN Controller
- Domande frequenti sui Wireless LAN Controller (WLC)
- ACL sui controller LAN wireless: regole, limitazioni ed esempi
- Esempio di configurazione dell'autenticazione Web esterna con i controller LAN wireless
- Esempio di configurazione dell'autenticazione Web del controller LAN wireless
- Esempio di configurazione di WLC, WLAN guest e WLAN interna
- Documentazione e supporto tecnico – Cisco Systems

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).