Accesso alla gestione per AireOS WLC tramite Server dei criteri di rete Microsoft

Sommario

Introduzione Prerequisiti Requisiti Componenti usati Premesse Configurazioni Configurazione WLC Configurazione Server dei criteri di rete Microsoft Verifica Risoluzione dei problemi

Introduzione

In questo documento viene descritto come configurare l'accesso alla gestione per la GUI e la CLI del WLC di AireOS tramite il Server dei criteri di rete Microsoft.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenza delle soluzioni per la sicurezza wireless
- Concetti su AAA e RADIUS
- Conoscenze base di Microsoft Server 2012
- Installazione di Server dei criteri di rete Microsoft e Active Directory (AD)

Componenti usati

Le informazioni fornite in questo documento si basano sui seguenti componenti software e hardware.

- Controller AireOS (5520) su 8.8.120.0
- Microsoft Server 2012

Nota: Questo documento ha lo scopo di fornire ai lettori un esempio della configurazione richiesta su un server Microsoft per l'accesso alla gestione WLC. La configurazione del server Microsoft Windows illustrata in questo documento è stata testata in laboratorio e ha funzionato come previsto. In caso di problemi con la configurazione, contattare Microsoft per assistenza. Il Cisco Technical Assistance Center (TAC) non supporta la configurazione del

server Microsoft Windows. Le guide all'installazione e alla configurazione di Microsoft Windows 2012 sono disponibili in Microsoft Tech Net.

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

Quando si accede alla CLI/GUI del WLC, all'utente viene richiesto di immettere le credenziali per eseguire correttamente l'accesso. È possibile verificare le credenziali rispetto a un database locale o a un server AAA esterno. In questo documento Microsoft Server dei criteri di rete viene utilizzato come server di autenticazione esterno.

Configurazioni

In questo esempio, due utenti sono configurati su AAA (NPS), ovvero **loginuser** e **adminuser**. **loginuser** dispone solo dell'accesso in sola lettura mentre **adminuser** dispone dell'accesso completo.

Configurazione WLC

Passaggio 1. Aggiungere il server RADIUS sul controller. Selezionare **Protezione > RADIUS > Autenticazione**. Fare clic su **Nuovo** per aggiungere il server. Verificare che l'opzione **management** sia abilitata in modo che il server possa essere utilizzato per l'accesso management, come mostrato nell'immagine.

| cisco | | <u>W</u> LANs | | WIRELESS | SECURITY | MANAGEMENT | COMMANDS | HELP | Se |
|---|--|---|---|---|----------------------|----------------------|-----------------|----------|-----------|
| Security | RADIUS | Authenti | ication Server | rs > Edit | | | | | |
| AAA General RADIUS Authentication Accounting Auth Cached Users Fallback DNS Downloaded AVP TACACS+ LDAP Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies Password Policies Local EAP Advanced EAP Priority Order Certificate Access Control Lists Wireless Protection Policies Web Auth TrustSec Local Policies Umbrella | Server In Server Ad Shared Si Shared Si Confirm S Key Wrap Apply Cis Apply Cis Port Num Server St Support fi Server Til Network I Managem Tunnel Pri Realm Lis PAC Provi IPSec Cisco ACA | dex ddress(Ipv4 ecret Formi ecret Shared Secr o co ISE Defa co ACA Def ber tatus for CoA meout User tent tent Retrans oxy t isioning | /Ipv6) at ret sult settings ault settings smit Timeout | 2 10.106.33.39 ASCII © (Designed fo 0 1812 Enabled © 5 secon ✓ Enable 5 second Enable Enable Enable | er FIPS custom ds | ers and requires a k | œy wrap complia | nt RADIU | S server; |
| Advanced | | | | | | | | | |

Passo 2: passare a **Sicurezza > Ordine di priorità > Utente di gestione**. Verificare che RADIUS sia selezionato come uno dei tipi di autenticazione.

| MONITOR | <u>W</u> LANs | CONTROLLER | WIRELESS | SECURITY | MANAGEMENT | | | | |
|----------------------------------|---------------|------------|----------|---------------|------------|--|--|--|--|
| Priority Order > Management User | | | | | | | | | |
| Authentic | ation | | | | | | | | |
| Not L | lsed | | Order U | sed for Authe | ntication | | | | |
| TACACS | + | > | | RADIUS | Up | | | | |
| | | < | | | Down | | | | |

Nota: Se si seleziona RADIUS come prima priorità nell'ordine di autenticazione, le credenziali locali verranno utilizzate per l'autenticazione solo se il server RADIUS non è raggiungibile. Se si seleziona RADIUS come seconda priorità, le credenziali RADIUS verranno innanzitutto verificate rispetto al database locale e quindi verificate rispetto ai server RADIUS configurati.

Configurazione Server dei criteri di rete Microsoft

Passaggio 1. Aprire il Server dei criteri di rete Microsoft. Fare clic con il pulsante destro del mouse

su Client Radius. Fare clic su New (Nuovo) per aggiungere il WLC come client RADIUS.

Immettere i dettagli richiesti. Verificare che il segreto condiviso sia uguale a quello configurato nel controller durante l'aggiunta del server RADIUS.

| • | WLC Properties X | x |
|-----------------------|--|---|
| File Action View Help | Settings Advanced Image: Enable this RADIUS client Image: Enable this RADIUS client Select an existing template: Image: Enable this RADIUS client Name and Address Friendly name: WLC Image: Enable this RADIUS client Address (IP or DNS): Image: Enable this RADIUS client Shared Secret Image: Enable this RADIUS client Shared Secret Image: Enable this RADIUS client with the same shared secret. click Generate are case-sensitive. Image: Enable this RADIUS client with the same shared secret. Client with the same shared secret. Shared secret: Image: Enable this RADIUS client with the same shared secret. Image: Enable this RADIUS client with the same shared secret. Image: Enable this RADIUS client with the same shared secret. Image: Enable this RADIUS client with the same shared secret. Image: Enable this RADIUS client with the same shared secret. Image: Enable this RADIUS client with the same shared secret. Image: Enable this RADIUS client with the same shared secret. Image: Enable this RADIUS client with the same shared secret. Image: Enable this RADIUS client with the same shared secret. Image: Enable this RADIUS client with the same shared secret. Image: Enable this RADIUS client with the same shared secret. Image: Enable this RADIUS client with this same shared secret. Image: Enable this RADIUS cli | |
| < III > | OK Cancel Apply | |

Passaggio 2. Passare a **Criteri > Criteri di richiesta di connessione**. Fare clic con il pulsante destro del mouse per aggiungere un nuovo criterio, come illustrato nell'immagine.

Passaggio 3. Nella scheda **Condizioni**, selezionare **Identificatore NAS** come nuova condizione. Quando richiesto, immettere il nome host del controller come valore, come mostrato nell'immagine.

| | Cisco WLC Properties | x |
|--|--|---|
| Overview Conditions Set | ttings | |
| Configure the conditions for If conditions match the con connection request, NPS s | r this network policy. Infection request, NPS uses this policy to authorize the connection request. If conditions do not match the kips this policy and evaluates other policies, if additional policies are configured. | |
| Condition | Value | |
| NAS Identifier | Cisco-WLC | |
| | | |
| Condition description: The NAS Identifier condition syntax to specify NAS name | n specifies a character string that is the name of the network access server (NAS). You can use pattern matching es. | |
| | Add Edit Remove |] |
| | OK Cancel Appl | y |

Passaggio 4. Passare a **Criteri > Criteri di rete**. Fare clic con il pulsante destro del mouse per aggiungere un nuovo criterio. In questo esempio, il criterio è denominato **Cisco WLC RW**, il che implica che il criterio venga utilizzato per fornire l'accesso completo (in lettura/scrittura). Verificare che il criterio sia configurato come illustrato di seguito.

| 0 | Cisco WLC RW Properties | × |
|--|---|---|
| File Action View Help File Action ACOUNTION File Action File Acti | Cisco WLC RW Properties Verview Conditions Constraints Settings Policy name: Policy State F enabled, NPS evaluates this policy while performing authorization. If disabled, NPS does not evaluate this policy. Policy state F enabled Access Pemission If conditions and constraints of the network policy match the connection request, the policy can either grant access or deny access. What is access permission? Grant access. Grant access if the connection request matches this policy. Policy and the policy grants access or deny access. Unhat is access of the connection request matches this policy. Policy and the policy grants access permission? Grant access. Grant access if the connection request matches this policy. Policy and the policy grants access, perform authorization with network policy only do net evaluate the dial-in properties of user accounts. Network connection method Select the type of network access server that sends the connection request to NPS. You can select either the network access server is an 802.1X authenticating switch or wireless access point, select Unspecified. Type of network access server: Dispecified V Vendor specific: Deny access server: Dispecified V Vendor specific: Deny access server: Dispecified V Vendor specific: Deny access server: Deny accesserve: Deny access server: Deny access server: Deny access serv | |
| < III > | OK Cancel Apply | , |

Passaggio 5. Nella scheda **Condizioni**, fare clic su **Aggiungi**. Selezionare i **gruppi di utenti** e fare clic su **Aggiungi**, come mostrato nell'immagine.

| Overview | Conditions | Constraints | Settings | | | | | | | | | |
|----------------------------|---|--|---------------------------------------|--|--|--|---------------------------------------|---|--------------------------|----------------------------|----------------|------|
| Configure | the condition | ns for this net | vork policy | | | | | | | | | |
| If condition connection | ns match the n request, N | Connection r PS skips this | equest, NF policy and | S uses this evaluates of | policy to au her policies | thorize the , if addition | connectional policies | on request. If are configure | conditio ed. | ns do not m | atch the | |
| | | | | | Select | conditi | on | | | | | x |
| Select | a condition, a | and then click | Add. | | | | | | | | | |
| Group | 05 | | | | | | | | | | | ^ |
| | Windows The Windo groups. Machine The Machi | Groups ws Groups c Groups ne Groups co | ondition sp andition sp | ecifies that | the connect | cting user | or compu uter must | ter must belo | ng to o e of the | ne of the se selected g | lected | Ξ |
| | User Gro The User (| ips Groups condi | tion specif | ies that the | connecting |) user mus | t belong t | o one of the s | elected | l groups. | | |
| | Location The HCAP required to network ac | Groups Location Gro match this p cess servers | oups condi olicy. The (NASs). S | tion specific HCAP proto See your NA | es the Host col is used S document | Credentia d for comm ntation bef | I Authoriz nunication ore using | ation Protoco between NP this condition | ol (HCA S and s n. | P) location ome third p | groups arty | ~ |
| | | | | | | | | | [| Add | Can | cel |
| | | | | | | | | Add | | Edit | Ren | nove |

Passaggio 6. Fare clic su **Add Groups** nella finestra di dialogo visualizzata. Nella finestra **Seleziona gruppo** visualizzata, selezionare il **tipo** e la **posizione** desiderati e immettere il nome dell'oggetto, come mostrato nell'immagine.

| | | Cisco WLC RW | Properties | s | |
|---------------------|---|-----------------------|------------|------------|-----------------------------------|
| hv | User G | roups | x | | |
| C Specify | y the group membership required | to match this policy. | | on reques | t. If conditions do not match the |
| Group | ps | | | | |
| | | | | | |
| | | | | iter must | belong to one of the selected |
| | Add Groups | Remove | | : belong t | o one of the selected groups. |
| | | ОК Са | ncel | o one of | the selected groups. |
| | Sel | ect Group | | | |
| Select th | is object type: | | | | ocol (HCAP) location groups |
| Group Error this | lacation: | | Object 1 | pes | tion. |
| wlanisc. | com | | Locatio | ns | Add Cancel |
| Enter the Domain | e object name to select (<u>examples</u> Admins |): | Check N | lames | |
| | | | | | Edit Remove |
| Adver | read | OK | C~ | land | |

La condizione, se aggiunta correttamente, dovrebbe essere simile a quella illustrata di seguito.

| | | | Cisco WLC RW Properties |
|---------------------------|---|--|---|
| verview | Conditions | Constraints | Settings |
| Configure If condition | the condition ons match the on request, N | ns for this network of the second sec | work policy. equest, NPS uses this policy to authorize the connection request. If conditions do not match the policy and evaluates other policies, if additional policies are configured. |
| Cor | ndition | V | alue |
| 🏭 Use | er Groups | W | /LANLSC\Domain Admins |
| | 4 | | |
| condition | description: | | |
| Condition The User | Groups cond | lition specifies | that the connecting user must belong to one of the selected groups. |
| Condition The User | Groups cond | ition specifies | a that the connecting user must belong to one of the selected groups. Add Edit Remove |

Nota: Per conoscere i dettagli relativi al percorso e al nome dell'oggetto, aprire Active Directory e cercare il nome utente desiderato. Nell'esempio, **Domain Admins** è costituito da utenti a cui è concesso l'accesso completo. **adminuser** fa parte del nome dell'oggetto.

| | Ac | tive Directory Use | rs and Con | nputers | | | - | x |
|--|--|--|--|---|---|----------------------------|---|----------------------|
| File Action View Help Active Directory Users and Com Active Directory Users and Com Saved Queries Wanlsc.com Builtin Computers Domain Controllers ForeignSecurityPrincipals Managed Service Accour Users | Admi Name Admi Admi Admi Admi Allow Anan AP US Ar US Ar US AC ert P AC Contr C | Remote control Member Of General Address Admin Use First name: Last name: Display name: Description: Office: | rs and Con Admin Us Remote D Dial-in Account er User Admin User | er Prope Desktop Sen Envir Profile | erties vices Profile onment Telephones | COM+ Sessions Organization | | × |
| < III > | St Doma Doma Doma Emple Enter; Coup Login RAS a Read- | Office: Telephone number: E-mail: Web page: | K C | ancel | Apply | Other Other | | |

| | Active | Directory | Users an | d Compute | rs | |
|--|---|--|---------------------------------|---|-------------------------------|--|
| File Action View Help | | Admin Us | ser Prop | erties | ? | × |
| Active Directory Users and Active Directory Users and Saved Queries Managed Service A Managed Service A Users | Remote control General Address Member Of Member of: Name Domain Admins | Remote Dial-in | Desktop Se Profile Envi | rvices Profile Telephones ronment | COM- Organizat Sessions | ion ion ro ro ro ro ro ro ro ro ro ro ro ro ro |
| | Primary group: [| Domain Admins There is n you have application | o need to o Macintosh ns. | change Primary (clients or POSI) | group unless K-compliant | ist ro ro ro |

Passaggio 7. Nella scheda Vincoli, passare a Metodi di autenticazione e accertarsi che sia selezionata solo l'autenticazione non crittografata.

| | Cisco WLC RW Properties |
|---|---|
| Overview Conditions Constraints Setting Configure the constraints for this network pol If all constraints are not matched by the conr Constraints: | s loy. rection request, network access is denied. |
| Authentication Methods Authentication Methods | Allow access only to those clients that authenticate with the specified methods. EAP types are negotiated between NPS and the client in the order in which they are listed. EAP Types: Move Up |
| NAS Port Type | Add Edt Remove Less secure authentication methods: |
| | User can change password after it has expired Microsoft Encrypted Authentication (MS-CHAP) User can change password after it has expired Encrypted authentication (CHAP) Unencrypted authentication (PAP, SPAP) Allow clients to connect without negotiating an authentication method Perform machine health check only |
| | OK Cancel Apply |

Passaggio 8. Nella scheda **Impostazioni**, selezionare **Attributi RADIUS > Standard**. Fare clic su **Add** per aggiungere un nuovo attributo, **Service-Type**. Dal menu a discesa, selezionare **Amministrativo** per fornire l'accesso completo agli utenti mappati a questo criterio. Fare clic su Applica per salvare le modifiche, come mostrato nell'immagine.

| tings: | | |
|---|--|-----------------------|
| ADIUS Attributes | Attribute Information | andard attribute, and |
| Standard | áttriku ta nama: | ADIUS clients. See |
| Vendor Specific | Service-Type | |
| etwork Access Protecti | Attribute number: | |
| NAP Enforcement | 6 | |
| Extended State | Attribute format: | |
| outing and Remote Acc | Enumerator | |
| Multilink and Bandwid Allocation Protocol (B | Attribute Value: Commonly used for Dial-Up or VPN | |
| P Filters | (none> V | |
| Encryption | Commonly used for 802.1x | |
| IP Settings | <pre></pre> | |
| | Others | |
| | Administrative | |
| | | |
| | OK Cancel | |
| | | |

Nota: Se si desidera concedere l'accesso in sola lettura a utenti specifici, selezionare NAS-Prompt dall'elenco a discesa. In questo esempio, viene creato un altro criterio denominato **Cisco WLC RO** per fornire l'accesso in sola lettura agli utenti sotto il nome oggetto **Domain Users**.

| | Cisco WLC RO Properties |
|---|---|
| Overview Conditions Constr | aints Settings |
| Configure the conditions for thi If conditions match the connec connection request, NPS skips | s network policy. tion request, NPS uses this policy to authorize the connection request. If conditions do not match the this policy and evaluates other policies, if additional policies are configured. |
| Condition | Value |
| all User Groups | WLANLSC\Domain Users |
| Condition description: The User Groups condition spe | ecifies that the connecting user must belong to one of the selected groups. |
| | OK Cancel Apply |

| | Cisco WLC RO Properties | X |
|---|--|---|
| Overview Conditions Const Configure the settings for this r If conditions and constraints m | aints Settings network policy. atch the connection request and the policy grants access, settings are applied. | |
| RADIUS Attributes | Attribute Information | _ |
| Standard Vendor Specific Network Access Protection | Attribute name: Service-Type Attribute number | |
| NAP Enforcement | 6 Attribute format: | |
| Routing and Remote Acc | Enumerator | |
| Multilink and Bandwid Allocation Protocol (B | Attribute Value: O Commonly used for Dial-Up or VPN | |
| TP Filters | (none> V | |
| Encryption | O Commonly used for 802.1x | |
| R IP Settings | <pre></pre> | |
| | Others | |
| | NAS Prompt V | |
| | OK Cancel | |
| | | |
| | | |

Verifica

1. Quando vengono utilizzate le credenziali **loginuser**, all'utente non è consentito configurare alcuna modifica sul controller.



| General | Security | QoS | Policy-Mapping | Advanced | | |
|------------|-----------------|-------|------------------------|---------------------|-------|---------|
| | | | | | | |
| Profile Na | ame | tes | tr | | | |
| Туре | | WL | AN | | | |
| SSID | SSID | | t2 | | | |
| Status | Status | | Enabled | | | |
| | | | | | | |
| Security | Policies | | | | | |
| | | | | | | inges.) |
| | | Autho | rization Failed. No su | fficient privileges | | |
| Radio Pol | icy | | | | | |
| Interface | /Interface Grou | | | | | |
| Multicast | Vlan Feature | | | | Close | |
| Broadcas | t SSID | 0 | Lilavieu | | | |
| NAS-ID | | nor | ne | | | |
| | | | | | | |
| | | | | | | |

Da **debug aaa all enable** è possibile verificare che il valore dell'attributo service-type nella risposta all'autorizzazione è 7, che corrisponde al prompt NAS.

```
*aaaQueueReader: Dec 07 22:20:14.664: 30:01:00:00:00:00 Successful transmission of
Authentication Packet (pktId 14) to 10.106.33.39:1812 from server queue 0, proxy state
30:01:00:00:00:00-00:00
*aaaQueueReader: Dec 07 22:20:14.664: 00000000: 01 0e 00 48 47 f8 f3 5c 58 46 98 ff 8e f8 20 7a
...HG..\XF....z
*aaaQueueReader: Dec 07 22:20:14.664: 00000010: f6 a1 f1 d1 01 0b 6c 6f 67 69 6e 75 73 65 72 02
.....loginuser.
*aaaQueueReader: Dec 07 22:20:14.664: 00000020: 12 c2 34 69 d8 72 fd 0c 85 aa af 5c bd 76 96 eb
...4i.r....\.v..
*aaaQueueReader: Dec 07 22:20:14.664: 00000030: 60 06 06 00 00 07 04 06 0a 6a 24 31 20 0b 43
....j$1..C
*aaaQueueReader: Dec 07 22:20:14.664: 00000040: 69 73 63 6f 2d 57 4c 43 isco-WLC
:
*radiusTransportThread: Dec 07 22:20:14.668: 30:01:00:00:00:00 Access-Accept received from
RADIUS server 10.106.33.39 (gid:0) with port:1812, pktId:14
*radiusTransportThread: Dec 07 22:20:14.668: AuthorizationResponse: 0xa3d3fb25a0
*radiusTransportThread: Dec 07 22:20:14.668: RadiusIndexSet(1), Index(1)
*radiusTransportThread: Dec 07 22:20:14.668:
protocolUsed.....0x0000001
*radiusTransportThread: Dec 07 22:20:14.668:
*radiusTransportThread: Dec 07 22:20:14.668: Packet contains 2 AVPs:
*radiusTransportThread: Dec 07 22:20:14.668: AVP[01] Service-
*radiusTransportThread: Dec 07 22:20:14.668: AVP[02]
Class.....DATA (44 bytes)
```

2. Quando vengono utilizzate le credenziali **adminuser**, l'utente deve disporre dell'accesso completo con il valore del **tipo di servizio** 6, che corrisponde a **amministrativo**.



```
*aaaQueueReader: Dec 07 22:14:27.439: AuthenticationRequest: 0x7fba240c2f00
*aaaQueueReader: Dec 07 22:14:27.439:
proxyState.....2E:01:00:00:00:00-00:00
*aaaQueueReader: Dec 07 22:14:27.439: Packet contains 5 AVPs:
*aaaQueueReader: Dec 07 22:14:27.439: AVP[01] User-Name......adminuser
(9 bytes)
*aaaQueueReader: Dec 07 22:14:27.439: AVP[04] Nas-Ip-
*aaaQueueReader: Dec 07 22:14:27.439: AVP[05] NAS-Identifier.....Cisco-WLC
(9 bytes)
:
:
*radiusTransportThread: Dec 07 22:14:27.442: 2e:01:00:00:00 Access-Accept received from
RADIUS server 10.106.33.39 (qid:0) with port:1812, pktId:13
*radiusTransportThread: Dec 07 22:14:27.442: AuthorizationResponse: 0xa3d3fb25a0
*radiusTransportThread: Dec 07 22:14:27.442:
protocolUsed.....0x00000001
*radiusTransportThread: Dec 07 22:14:27.442:
proxyState.....2E:01:00:00:00:00-00:00
*radiusTransportThread: Dec 07 22:14:27.442: AVP[01] Service-
Type.....0x00000006 (6) (4 bytes)
*radiusTransportThread: Dec 07 22:14:27.442: AVP[02]
Class.....DATA (44 bytes)
```

Risoluzione dei problemi

Per risolvere i problemi di accesso alla gestione di WLC tramite Server dei criteri di rete, eseguire il comando **debug aaa all enable**.

1. Di seguito sono riportati i log in caso di utilizzo di credenziali errate.

*aaaQueueReader: Dec 07 22:36:39.753: 32:01:00:00:00:00 Successful transmission of Authentication Packet (pktId 15) to 10.106.33.39:1812 from server queue 0, proxy state 32:01:00:00:00:00-00:00 *aaaQueueReader: Dec 07 22:36:39.753: 00000000: 01 0f 00 48 b7 e4 16 4d cc 78 05 32 26 4c ec 8dH....M.x.2&L... *aaaQueueReader: Dec 07 22:36:39.753: 00000010: c7 a0 5b 72 01 0b 6c 6f 67 69 6e 75 73 65 72 02 ..[r..loginuser. *aaaQueueReader: Dec 07 22:36:39.753: 00000020: 12 03 a7 37 d4 c0 16 13 fc 73 70 df 1f de e3 e47.....sp..... *aaaQueueReader: Dec 07 22:36:39.753: 00000030: 32 06 06 00 00 07 04 06 0a 6a 24 31 20 0b 43 2....j\$1..C *aaaQueueReader: Dec 07 22:36:39.753: 00000040: 69 73 63 6f 2d 57 4c 43 isco-WLC *aaaQueueReader: Dec 07 22:36:39.753: 32:01:00:00:00:00 User entry not found in the Local FileDB for the client. *radiusTransportThread: Dec 07 22:36:39.763: 32:01:00:00:00:00 Counted 0 AVPs (processed 20 bytes, left 0) *radiusTransportThread: Dec 07 22:36:39.763: 32:01:00:00:00:00 Access-Reject received from

RADIUS server 10.106.33.39 (qid:0) with port:1812, pktId:15

*radiusTransportThread: Dec 07 22:36:39.763: 32:01:00:00:00 Did not find the macaddress to be deleted in the RADIUS cache database

*radiusTransportThread: Dec 07 22:36:39.763: 32:01:00:00:00:00 Returning AAA Error

'Authentication Failed' (-4) for mobile 32:01:00:00:00 serverIdx 1

*radiusTransportThread: Dec 07 22:36:39.763: AuthorizationResponse: 0x7fbaebebf860

*radiusTransportThread: Dec 07 22:36:39.763: structureSize......136

*radiusTransportThread: Dec 07 22:36:39.763: resultCode.....-4

*radiusTransportThread: Dec 07 22:36:39.763:

protocolUsed.....0xfffffff

*radiusTransportThread: Dec 07 22:36:39.763: Packet contains 0 AVPs:

*emWeb: Dec 07 22:36:39.763: Authentication failed for loginuser

2. I registri quando service-type viene utilizzato con un valore diverso da Administrative (valore=6) o NAS-prompt (valore=7) vengono visualizzati come segue. In questo caso, l'accesso non riesce anche se l'autenticazione ha esito positivo.

```
*aaaQueueReader: Dec 07 22:46:31.849: AuthenticationRequest: 0x7fba240c56a8
*aaaQueueReader: Dec 07 22:46:31.849:
*aaaQueueReader: Dec 07 22:46:31.849: Packet contains 5 AVPs:
*aaaQueueReader: Dec 07 22:46:31.849: AVP[01] User-Name......adminuser
(9 bytes)
*aaaQueueReader: Dec 07 22:46:31.849: AVP[03] Service-
Type.....0x00000007 (7) (4 bytes)
*aaaQueueReader: Dec 07 22:46:31.849: AVP[04] Nas-Ip-
*aaaQueueReader: Dec 07 22:46:31.849: AVP[05] NAS-Identifier.....Cisco-WLC
(9 bytes)
:
:
*radiusTransportThread: Dec 07 22:46:31.853: AuthorizationResponse: 0xa3d3fb25a0
*radiusTransportThread: Dec 07 22:46:31.853: RadiusIndexSet(1), Index(1)
*radiusTransportThread: Dec 07 22:46:31.853: resultCode.....0
*radiusTransportThread: Dec 07 22:46:31.853:
protocolUsed.....0x00000001
*radiusTransportThread: Dec 07 22:46:31.853: Packet contains 2 AVPs:
*radiusTransportThread: Dec 07 22:46:31.853: AVP[01] Service-
Type.....0x00000001 (1) (4 bytes)
*radiusTransportThread: Dec 07 22:46:31.853: AVP[02]
Class.....DATA (44 bytes)
*emWeb: Dec 07 22:46:31.853: Authentication succeeded for adminuser
```