Microsoft NPS를 통한 AireOS WLC에 대한 관리 액세스

목차

소개 <u>사전 요구 사항</u> <u>요구 사항</u> <u>사용되는 구성 요소</u> <u>배경 정보</u> <u>구성</u> <u>WLC 컨피그레이션</u> <u>Microsoft NPS 구성</u> <u>다음을 확인합니다.</u> <u>문제 해결</u>

소개

이 문서에서는 Microsoft NPS(Network Policy Server)를 통해 AireOS WLC GUI 및 CLI에 대한 관리 액세스를 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- 무선 보안 솔루션 지식
- AAA 및 RADIUS 개념
- Microsoft Server 2012에 대한 기본 지식
- Microsoft NPS 및 AD(Active Directory) 설치

사용되는 구성 요소

이 문서에서 제공하는 정보는 다음 소프트웨어 및 하드웨어 구성 요소를 기반으로 합니다.

- 8.8.120.0의 AireOS 컨트롤러(5520)
- Microsoft Server 2012

참고:이 문서는 WLC 관리 액세스를 위해 Microsoft 서버에 필요한 구성의 예를 독자에게 제공 하기 위한 것입니다.이 문서에 제시된 Microsoft Windows 서버 구성은 Lab에서 테스트되었으 며 예상대로 작동하는 것으로 확인되었습니다.구성에 문제가 있으면 Microsoft에 도움을 요청 하십시오.Cisco TAC(Technical Assistance Center)는 Microsoft Windows 서버 구성을 지원하 지 않습니다.Microsoft Windows 2012 설치 및 구성 가이드는 Microsoft Tech Net에서 찾을 수 있습니다. 이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바 이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

WLC CLI/GUI에 액세스하면 사용자에게 성공적으로 로그인하기 위한 자격 증명을 입력하라는 프 롬프트가 표시됩니다.로컬 데이터베이스 또는 외부 AAA 서버에 대해 자격 증명을 확인할 수 있습 니다.이 문서에서 Microsoft NPS는 외부 인증 서버로 사용되고 있습니다.

구성

이 예에서는 AAA(NPS) 뷰에 두 명의 사용자가 구성됩니다. loginuser와 adminuser입니다. .loginuser는 읽기 전용 액세스 권한만 가지며 administrator는 전체 액세스 권한을 갖습니다.

WLC 컨피그레이션

1단계. 컨트롤러에 RADIUS 서버를 추가합니다.Security(**보안) > RADIUS > Authentication(인증)으 로 이동합니다**.New(**새로 만들기**)를 클릭하여 서버를 추가합니다.이 이미지에 표시된 대로 이 서버 를 관리 액세스에 사용할 수 있도록 관리 옵션이 활성화되어 있는지 확인합니다.

cisco		<u>W</u> LANs	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	Sa EEEDB
Security	RADIUS	Authenti	cation Server	rs > Edit					
AAA General RADIUS Authentication Accounting Auth Cached Users Fallback DNS Downloaded AVP TACACS+ LDAP	Server In Server Ad Shared Se Shared Se Confirm S Key Wrap	dex ddress(Ipv4 ecret Forma ecret Shared Secr	/Ipv6) at ret	2 10.106.33.3 ASCII 0 ••• •••	9 or FIPS custom	ers and requires a l	vey wrap complia	nt RADIU	S server!
LDAP Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies Password Policies	Apply Cis Apply Cis Port Num	co ISE Defa co ACA Def ber	ault settings	(Designed 7 1812 Enabled 7	or rara costorn	ers and requires a r	кеу итар сопрна		o server,
Local EAP	Support f	or CoA		Disabled C					
Advanced EAP Priority Order	Server Tir Network	meout User		5 secor	nds				
Certificate Access Control Lists	Managem	ient ient Retran	smit Timeout	✓ Enable	ds				
Wireless Protection Policies	Tunnel Pr	оху		Enable					
Web Auth TrustSec	PAC Provi	isioning		Enable					
Local Policies Umbrella	Cisco ACA			Enable					

Advanced

2단계. **보안 > 우선순위 주문 > 관리 사용자로 이동합니다**.RADIUS가 인증 유형 중 하나로 선택되 었는지 확인합니다.

MONITOR	<u>W</u> LANs	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT
Priority C	order > N	lanagement l	Jser		
Authentic	ation				
Not	Used		Order U	sed for Authe	entication
TACACS	5+	>		RADIUS	Up
		<			Down

참고:RADIUS를 인증 순서의 첫 번째 우선 순위로 선택한 경우 로컬 자격 증명은 RADIUS 서 버에 연결할 수 없는 경우에만 인증에 사용됩니다.RADIUS를 두 번째 우선 순위로 선택한 경 우 먼저 로컬 데이터베이스에 대해 RADIUS 자격 증명을 확인한 다음 구성된 RADIUS 서버에 대해 확인합니다.

Microsoft NPS 구성

1단계. Microsoft NPS 서버를 엽니다.Radius 클라이언트를 마우스 오른쪽 버튼으로 **클릭합니다** .New(**새로 만들기**)를 클릭하여 WLC를 RADIUS 클라이언트로 추가합니다.

필요한 세부사항을 입력합니다.RADIUS 서버를 추가하는 동안 공유 암호가 컨트롤러에 구성된 암 호와 동일한지 확인하십시오.

	WLC Properties	x
File Action View Help File Action View Help NPS (Local) RADIUS Clients and Servers RADIUS Clients RADIUS Clients Remote RADIUS Server Policies Network Access Protection Accounting Templates Management	WLC Properties X Settings Advanced P Enable this RADIUS client Select an existing template: Select an existing template: V Name and Address Friendy name: WLC Address (IP or DNS): WLC Verfy Shared Secret Select an existing Shared Secrets template: None V To manually type a shared secret, click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared secret entered here. Shared secrets are case-sensitive. Manual Generate Shared secret: Confirm shared secret: Confirm shared	×
	OK Cancel Apply	

2단계. Policies(정책) **> Connection Request Policies(연결 요청 정책)로 이동합니다**.이미지에 표시 된 대로 새 정책을 추가하려면 마우스 오른쪽 버튼을 클릭합니다.

•	Cisco WLC Properties	~
File Action View Help	Overview Conditions Settings Policy name: Disco WLC	1
 NPS (Local) RADIUS Clients and Servers RADIUS Clients Remote RADIUS Server Policies Connection Request Po Network Policies Health Policies Network Access Protection System Health Validato Remediation Server Gro Accounting Templates Management 	Policy State If enabled, NPS evaluates this policy while processing connection requests. If disabled, NPS does not evalue this policy. Policy enabled 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 type or Vendor specific, but nether is required. If your network access server is an 802.1X authenticating switch or wireless access point, select Unspecified. Type of network access server: Unspecified Vendor specific:	
К Ш У	OK Cancel Apply	

3단계. Conditions 탭에서 NAS Identifier를 새 조건으로 선택합니다.프롬프트가 표시되면 이미지에 표시된 대로 컨트롤러의 호스트 이름을 값으로 입력합니다.

	Cisco WLC Properties	x
Overview Conditions Settings Configure the conditions for this	network policy.	
If conditions match the connect connection request, NPS skips	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	
NAS Identifier	Cisco-WLC	
Condition description:		-
The NAS Identifier condition sp syntax to specify NAS names.	ecifies a character string that is the name of the network access server (NAS). You can use pattern matching	
	Add Edit Remove	
		-
L		
	OK Cancel App	NY

4단계. Policies(정책) > Network Policies(네트워크 정책)로 이동합니다.마우스 오른쪽 버튼을 클릭 하여 새 정책을 추가합니다.이 예에서 정책 이름은 Cisco WLC RW로 지정되며, 이는 정책이 전체 (읽기-쓰기) 액세스를 제공하는 데 사용됨을 의미합니다.여기에 표시된 대로 정책이 구성되어 있는 지 확인합니다.

0	Cisco WLC RW Properties	X
File Action View Help File Action View Help File Action View Help File Action View Help Action Constant Constant File Action View Help File Action Constant	Cisco WLC RW Properties Overview Conditions Constraints Settings Policy name: Seco WLC RW Policy State If enabled, NPS evaluates this policy while performing authorization. If disabled, NPS does not evaluate this policy. If enabled Access Permission	
 Health Policies Network Access Protection Accounting Templates Management 	If conditions and constraints of the network policy match the connection request, the policy can either grant access or deny access. <u>What is access permission?</u>	
	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 type or Vendor specific, but neither is required. If your network access server is an 802.1X authenticating switch or wireless access point, select Unspecified. Type of network access server: Unspecified Vendor specific: 10	
< III >	OK Cancel Appl	y

5단계. Conditions 탭에서 Add를 클릭합니다.사용자 그룹을 선택하고 이미지에 표시된 대로 Add를 클릭합니다.

	Cisco WLC RW Properties	
Overview	Conditions Constraints Settings	
Configure	he conditions for this network policy.	
If condition connection	is match the connection request, NPS uses this policy to authorize the connection request. If conditions do not match the request, NPS skips this policy and evaluates other policies, if additional policies are configured.	
	Select condition	x
Select	condition, and then click Add.	
Group	3	^
1	Windows Groups The Windows Groups condition specifies that the connecting user or computer must belong to one of the selected groups.	=
	Machine Groups The Machine Groups condition specifies that the connecting computer must belong to one of the selected groups.	
Sec.	User Groups The User Groups condition specifies that the connecting user must belong to one of the selected groups.	
	Location Groups The HCAP Location Groups condition specifies the Host Credential Authorization Protocol (HCAP) location groups required to match this policy. The HCAP protocol is used for communication between NPS and some third party network access servers (NASs). See your NAS documentation before using this condition.	~
	Add Can	cel
	Add Edit Ren	iove

6단계. 대화 상자에서 Add Groups(그룹 추가)를 클릭합니다.나타나는 그룹 선택 창에서 원하는 객 체 유형 및 위치를 선택하고 이미지에 표시된 대로 필요한 객체 이름을 입력합니다.

	Cisco WLC RW Prope	erties	5		L
v	User Groups	x			
C If	Specify the group membership required to match this policy.		on reques	t. If conditions do not match the	
×	Groups		are conf	igured.	x
				-	
			iter must	belong to one of the selected	1
	Add Groups Remove		: belong t	o one of the selected groups.	
Ļ	OK Cancel		o one of	the selected groups.	
	Select this object type:			col (HCAP) location groups	
	Group	ect Ty	pes	NPS and some third party tion.	
	From this location:			<u> </u>	
	wlanisc.com	ocation	ns	Add Cancel	
	Enter the object name to select (examples): Domain Admins Ch	eck Ni	ames	Edit Remove	
	Advanced OK	Can	cel		

조건을 올바르게 추가한 경우 여기에 표시된 대로 확인해야 합니다.

			Cisco WLC RW Properties
verview	Conditions	Constraints	Settings
Configure If conditio connectio	the condition ns match the on request, N	connection r PS skips this p	work policy. request, 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	dtion	Va	alue
🚜 Use	r Groups	W	/LANLSC\Domain Admins
Condition	description:	itinn enartiae	s that the connection user must helped to one of the selected omune
Condition The User	description: Groups cond	lition specifies	s that the connecting user must belong to one of the selected groups. Add Edt

참고:위치 및 객체 이름 세부 정보를 확인하려면 active directory를 열고 원하는 사용자 이름을 찾습니다.이 예에서 Domain Admins은 전체 액세스 권한을 가진 사용자로 구성됩니다 .adminuser는 이 개체 이름의 일부입니다.

	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 and Computers	
File Action View Help	Admin User Properties ? X	
Active Directory Users and Active Directory Users and Saved Queries Managed Service A Users	Remote control Remote Desktop Services Profile COM+ General Address Account Profile Telephones Organization Member Of Dial-in Environment Sessions Member of:	
	Primary group: Domain Admins Set Primary Group There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications.	

7단계. Constraints 탭에서 Authentication Methods(인증 방법)로 이동하고 **암호화되지 않은 인증만** 선택했는지 확인합니다.

Overview Conditions Constraints Settings Configure the constraints for this network policy. If all constraints are not matched by the connection request, network access is denied. Constraints: Constraints Image: Constraints Authentication Methods Image: Called Station ID Move Up Image: Called Station ID Move Down Image: Called Station ID		Cisco WLC RW Properties
Add Edit Remove	Overview Conditions Constraints Setting Configure the constraints for this network polified constraints are not matched by the constraints: Constraints Constraints: Constraints Muthentication Methods Image: Constraints Idle Timeout Session Timeout Called Station ID Oay and time restrictions NAS Port Type	Cisco WLC RW Properties X ps Nicy. nection request, network access is denied. X Allow access only to those clients that authenticate with the specified methods. X EAP types are negotiated between NPS and the client in the order in which they are listed. Move Up EAP Types: Move Up Move Down Move Down
 Microsoft Encrypted Authentication version 2 (MS-CHAP-v2) 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 		Add Edit Remove Less secure authentication methods: Microsoft Encrypted Authentication version 2 (MS-CHAP-v2) 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

8단계. Settings(설정) 탭 아래에서 RADIUS Attributes(RADIUS 특성) > Standard(표준)로 이동합니 다.Add(추가)를 클릭하여 새 특성, Service-Type을 추가합니다.드롭다운 메뉴에서 Administrative(관리)를 선택하여 이 정책에 매핑된 사용자에 대한 전체 액세스를 제공합니다.이미 지에 표시된 대로 Apply(적용)를 클릭하여 변경 사항을 저장합니다.

ttings: RADIUS Attributes	Attribute Information X	
Standard Standard Vendor Specific Network Access Protection NAP Enforcement Extended State Routing and Remote Acce Multilink and Bandwid Allocation Protocol (B) IP Filters	Attribute information andard attribute information Attribute name: Service-Type Attribute number: 6 Attribute format: Enumerator Attribute Value: O Commonly used for Dial-Up or VPN	xute, and its. See
A Encryption	 Commonly used for 802.1x Image: Conness ✓ Others OK Cancel 	

참고:특정 사용자에게 읽기 전용 액세스를 제공하려면 드롭다운에서 NAS-Prompt를 선택합 니다.이 예에서는 Domain Users 객체 이름 아래**에** 사용자에게 읽기 전용 액세스를 제공하기 위해 **Cisco WLC RO**라는 다른 정책이 생성됩니다.

	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 Constru	aints Settings	_
Configure the settings for this n If conditions and constraints m	etwork policy. atch the connection request and the policy grants access, settings are applied.	
Settings:		_
RADIUS Attributes	Attribute Information and attribute, and	
Vendor Specific	Attribute name: Service-Type	
Network Access Protecti	Attrbute number:	
NAP Enforcement	6	
Extended State	Attribute format:	
Routing and Remote Acc	Enumerator	
Multilink and Bandwid Allocation Protocol (B	Attribute Value: O Commonly used for Dial-Up or VPN	
IP Filters	(none>	
Encryption	O Commonly used for 802.1x	
A IP Settings	(none>	
	Others	
	NAS Prompt	
	OK Cancel	
	OK Cancel Apph	,

다음을 확인합니다.

1. 로그인 사용자 자격 증명을 사용할 때 사용자는 컨트롤러에서 변경 사항을 구성할 수 없습니다.



ieneral	Security	QoS	Policy-Mapping	Advanced		
Profile Na	ame	tes	str			
Туре		WL	AN			
SSID		tes	st2			
Status			Enabled			
Security	Policies					inges.)
Security Radio Po	Policies	Autho	rization Failed. No su	fficient privileges	5	inges.)
Security Radio Pol Interface	Policies licy c/Interface Grou	Autho	prization Failed. No su	fficient privileges	5	inges.)
Security Radio Pol Interface Multicast	Policies licy /Interface Grov	Autho	prization Failed. No su	fficient privileges	s Close	inges.)
Security Radio Pol Interface Multicast Broadcas	Policies licy /Interface Grou Vlan Feature et SSID	Autho	prization Failed. No su	fficient privileges	s Close	inges.)

debug **aaa all enable**에서 권한 부여 응답에서 service-type 특성의 값이 NAS 프롬프트에 해당하는 7임을 확인할 수 있습니다.

```
*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
\dots HG. \backslash 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 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 (qid: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-
Type.....0x00000007 (7) (4 bytes)
*radiusTransportThread: Dec 07 22:20:14.668: AVP[02]
Class.....DATA (44 bytes)
2. 관리자 자격 증명을 사용하는 경우 사용자는 관리에 해당하는 서비스 유형 값 6의 모든 액세스 권
```

한을 가지고 있어야 합니다.



```
*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)
```

문제 해결

NPS를 통해 WLC에 대한 관리 액세스 문제를 해결하려면 debug aaa all enable 명령을 실행합니다

1. 잘못된 자격 증명이 사용된 로그는 여기에 표시됩니다.

*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 8d ...H...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 32:01:00:00:00:00 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. service-type이 Administrative(값=6) 이외의 값 또는 NAS 프롬프트(값=7)가 아닌 값과 함께 사용 되는 로그는 다음과 같습니다.이러한 경우 인증이 성공하더라도 로그인이 실패합니다.

```
*aaaQueueReader: Dec 07 22:46:31.849: AuthenticationRequest: 0x7fba240c56a8
*aaaQueueReader: Dec 07 22:46:31.849: Callback.....0xa3c13ccb70
*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-
*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.....0x0000001
*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
```