通過Microsoft NPS對AireOS WLC的管理訪問

目錄

<u>簡介</u> <u>必要條件</u> <u>需求</u> <u>採用元件</u> <u>背景資訊</u> <u>組態</u> <u>WLC組態</u> <u>Microsoft NPS配置</u> <u>驗證</u> 疑難排解

簡介

本文說明如何通過Microsoft網路策略伺服器(NPS)為AireOS WLC GUI和CLI配置管理訪問。

必要條件

需求

思科建議您瞭解以下主題:

- 無線安全解決方案知識
- AAA和RADIUS概念
- Microsoft Server 2012基礎知識
- 安裝Microsoft NPS和Active Directory(AD)

採用元件

本文檔中提供的資訊基於以下軟體和硬體元件。

- 8.8.120.0上的AireOS控制器(5520)
- Microsoft Server 2012

附註:本文旨在為讀者提供在Microsoft伺服器上進行WLC管理訪問所需的配置示例。本文檔 中介紹的Microsoft Windows伺服器配置已在實驗室中經過測試,發現可以按預期工作。如果 配置有問題,請與Microsoft聯絡以獲得幫助。思科技術支援中心(TAC)不支援Microsoft Windows伺服器配置。Microsoft Windows 2012安裝及設定指南可在Microsoft Tech Net上找 到。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除(預設))的組態來啟動。如果您的網路正在作用,請確保您已瞭解任何指令可能造成的影響。

背景資訊

訪問WLC CLI/GUI時,系統會提示使用者輸入憑證以成功登入。可以針對本地資料庫或外部AAA伺服器驗證憑證。在本文檔中,Microsoft NPS用作外部身份驗證伺服器。

組態

在本範例中,在AAA(NPS)上設定兩個使用者,即**loginuser**和**adminuser**。**loginuser只**有只讀訪問許 可權,而adminuser獲**得完**整訪問許可權。

WLC組態

步驟1.在控制器上新增RADIUS伺服器。導覽至Security > RADIUS > Authentication。按一下 New新增伺服器。確保啟用了management選項,以便此伺服器可用於管理訪問,如下圖所示。

cisco		<u>W</u> LANs	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	Sa EEEDB
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 Priority Order Certificate Access Control Lists Wireless Protection Policies Web Auth TrustSec Local Policies Umbrelia 	Server In Server Ad Shared Si Shared Si Confirm S Key Wrap Apply Cis Port Num Server St Support fi Server Tit Network I Managem Tunnel Pin Realm Lis PAC Provi IPSec Cisco ACA	dex dress(Ipv4 ecret Forma ecret shared Secr co ISE Defa co ISE Defa co ACA Def ber atus or CoA meout User ent ent Retrans oxy sioning	/Ipv6) at ret ault settings ault settings	2 10.106.33.3 ASCII © (Designed for 1812 Enabled © 5 secon Ø Enable Enable Enable Enable Enable	9 or FIPS custom ds	ers and requires a k	ey wrap complia	nt RADIU	S server;
h Advanced									

步驟2.定位至安全性>優先順序順序>管理使用者。確保RADIUS被選為其中一個身份驗證型別。

MONITOR	<u>W</u> LANs	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	
Priority Order > Management User						
Authentica	ntion		Order II	end for Author	ntication	
NOLO	seu		order of	seu for Authe	nucation	
TACACS	+	>		LOCAL	Up	
		<			Down	

附註:如果選擇RADIUS作為身份驗證順序中的第一個優先順序,則只有在RADIUS伺服器無 法訪問時,才會使用本地憑據進行身份驗證。如果選擇RADIUS作為第二個優先順序,將首先 針對本地資料庫驗證RADIUS憑證,然後針對配置的RADIUS伺服器進行檢查。

Microsoft NPS配置

步驟1.開啟Microsoft NPS伺服器。按一下右鍵**Radius Clients**。按一下「**New**」,將WLC新增為 RADIUS使用者端。

輸入所需的詳細資訊。請確認增加RADIUS伺服器時,共用密碼與控制器上設定的密碼相同。

	WLC Properties	×	x
File Action View Help	Settings Advanced Image: Select an existing template: Image: Select an existing template: Name and Address Friendly name: WLC Address (IP or DNS): Address (IP or DNS): Image: Select an existing Shared Secrets template: None Shared Secret Select an existing Shared Secrets template: None To manually type a shared secret, click Manual. To automatically ger secret, click Generate. You must configure the RADIUS client with the secret entered here. Shared secrets are case-sensitive. Image: Manual Shared secret: Image: Shared secret: Image: Confirm shared secret: Image: Shared secret: Image: OK OK	Verfy Verfy	

步驟2.導航到Policies > Connection Request Policies。按一下右鍵可新增新策略,如下圖所示。

•	Cisco WLC Properties
File Action View Help	Overview Conditions Settings
🗢 🔿 🙍 🖬 🖬 👘	Policy name: Daco WLC
 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 	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.
Remediation Server Gro	Uppe of network access server.
Templates Management	O Vendor specific:
< III >	OK Cancel Apply

步驟3.在Conditions頁籤下,選擇NAS Identifier作為新條件。出現提示時,輸入控制器的主機名作 為值,如下圖所示。

	Cisco WLC Properties	x
Overview Conditions Settings	1	
Configure the conditions for this If conditions match the connecti connection request, NPS skips t	network policy. on request, NPS uses this policy to authorize the connection request. If conditions do not match the his policy and evaluates other policies, if additional policies are configured.	
Condition	Value	
🛣 NAS Identifier	Cisco-WLC	
Condition description: The NAS Identifier condition spe 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	
	OK Cancel Ap	ply

步驟4.導覽至Policies > Network Policies。按一下右鍵可新增新策略。在本例中,策略名稱為Cisco WLC RW,這表示策略用於提供完全(讀取/寫入)訪問許可權。確保策略配置如圖所示。

File Action View Help Verview Constraints Settings Policy State Policy State Policy State Fenabled, NPS valuates this policy while performing authorization. If disabled, NPS does not evaluate this policy. Policy State Fenabled, NPS evaluates this policy while performing authorization. If disabled, NPS does not evaluate this policy. Policy State Fenabled, NPS evaluates this policy while performing authorization. If disabled, NPS does not evaluate this policy. Policy Brate Fenabled -Access Permission If conditions and constraints of the network policy match the connection request, the policy can either grant access or deny access. While is access permission? • Network Access Protection • Recounting • Templates Management • Grant access. Grant access if the connection request matches this policy. • Ignore user account dial in properties. • Head on the network policy only: do not evaluate the dail in properties of user accounts. • Network connection method Select the type of network access server: • Unspecified • Unspecified • Unspecified • Vendor specific: • Unspecified • Vendor specific: • Unspecified • Vendor specific: • Vendor spe	0	Cisco WLC RW Properties	×
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. Image: Type of network access server: Unspecified v Vendor specific: 10 Image: Type of network access server: 10 Image: Type of network accesserver 10	File Action View Help Image: State	Cisco WLC RW Properties Overview Conditions Constraints Settings Policy name: Disco WLC RW Policy State If enabled, NPS evaluates this policy while performing authorization. If disabled, NPS does not evaluate this policy. Policy enabled Access Permission 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. Deny access if the connection request matches this policy. Ignore user account dial-in properties. If the connection request matches the constraints of this network policy and the policy grants access, perform authorization with network policy only; do not evaluate the dial-in properties of user accounts . 	
OK Califer Apply	< III >	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. Image: Type of network access server: Unspecified v Vendor specific: Image: Type of network access server: Unspecified v OK Cancel	

步驟5.在Conditions索引標籤下,按一下Add。選擇User groups,然後按一下Add,如下圖所示。

					Cis	sco W	LC R	W Pr	opert	ties								L
Overview	Conditions	Constraints	Settings															
Configure	the condition	ns for this netw	vork policy															
If conditio	ons match the on request, N	connection r PS skips this ;	equest, NP policy and (^o S use evalua	es this lates of	policy t ther po	to auth licies, if	orize th f additio	e conn onal pol	ection licies a	n requ are ci	uest. If c onfigure	condit ed.	ions de	o not ma	atch the		
						Sel	ect c	ondit	ion									X
Select	a condition, a	and then click	Add.															
Group	ps																	^
10	Windows The Windo groups.	Groups ws Groups c	ondition sp	pecifie	es that	t the co	onnecti	ing use	r or co	mpute	er mu	ist belo	ng to	one of	the sel	ected		Ξ
HCAF	User Grou	ne Groups co Ips Groups condi	ndition sp tion specif	ecifie fies th	as that	the co	nnectir cting u	ng com Iser mu	puter r	must b	one	g to one of the s	e of th	e sele ed gro	ups.	oups.		
	Location The HCAP required to network ac	Groups Location Gro match this p ccess servers	oups condi olicy. The (NASs). S	tion s HCAF See yo	P proto our N/	ies the ocol is AS doc	Host C used f umenta	redent or com ation b	ial Aut munica efore u	horiza ation sing t	ation betwee this c	Protoco een NP: onditior	ol (HC S and n.	AP) Id some	third p	groups arty		~
														1	\dd	(Cancel	
												Add		E	dit	F	Remove	•

步驟6.在出現的對話方塊中按一下Add Groups。在出現的選擇組視窗中,選擇所需的對象型別和位置,然後輸入所需的對象名稱,如下圖所示。

Cisco WLC R	W Propertie	S	
User Groups	x		
Specify the group membership required to match this policy.		on reque	st. If conditions do not match the
Groups		are con	figured.
			_
			_
		iter must	t belong to one of the selected
Add Groups Remo	ve	belong	to one of the selected groups.
ОК	Cancel	io one of	the selected groups.
Select Group		×	
Select this object type:	Object T	imee	ocol (HCAP) location groups NPS and some third party
From this location:	Object	урсэ	tion.
wlanlsc.com	Locatio	ons	Add Cancel
Enter the object name to select (examples):			Caroor
Domain Admins	Check 1	lames	Edit Remove
Advanced	K Ca	ncel	

如果條件新增正確,應如下所示。

			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

附註:要瞭解位置和對象名稱的詳細資訊,請開啟Active Directory並查詢所需的使用者名稱。 在本示例中,**域管理員**由具有完全訪問許可權的使用者組成。**adminuser是**此對象名稱的一部 分。

	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 AP US AC Contr AC Contr AC Contr AC Contr AC Doma A Doma A Doma A Doma A Doma A Doma A Doma A Doma A Doma A Doma A Doma A Doma A Doma A Doma A Doma A Doma A Doma A Doma	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		

File Action View Help Admin User Properties ?		Active	Directory	Users ar	nd Compute	ers	
Active Directory Users and Remote control Remote Desktop Services Profile COM Saved Queries Manlsc.com Member Of Dial-in Environment Sessions Soved Soverse Domain Controller: Domain Controller: Member of: Name Active Directory Domain Services Folder Managed Service A Wers Vsers Managed Service A Memore Add Remove Primary group: Domain Admins Memore Set Primary Group There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications.	File Action View Help		Admin U	ser Prop	erties	?	×
Add Remove Primary group: Domain Admins Set Primary Group There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications.	Active Directory Users and Saved Queries Saved Qu	Remote control General Address Member Of Member of: Name Domain Admins	Remote I Account Dial-in Active Direct wlanlsc.com/	Desktop Se Profile Env ory Domain /Users	rvices Profile Telephones ironment	COM+ Organizati Sessions	on prac rou rou rou rou rou s G re p istra
OK Cancel Apply Help		Add Primary group: Set Primary Group	Remove Domain Admins There is n you have applicatio	no need to Macintosh ns. Cancel	change Primary clients or POSIX	group unless X-compliant	istra rou or g

步驟7.在Constraints索引標籤下,導覽至Authentication Methods,並確保僅勾選未加密的驗證。

	Cisco WLC RW Properties
Overview Conditions Constraints Setting Configure the constraints for this network polif all constraints are not matched by the constraints: Constraints Constraints: Constraints Constraints: Authentication Methods Image: Session Timeout Session Timeout Image: Called Station ID Day and time restrictions Image: NAS Port Type NAS Port Type	Cisco WLC RW Properties s Icy. nection request, network access is denied. 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 Move Down
	Add Edt 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 How clients to connect without negotiating an authentication method Perform machine health check only
	OK Cancel Apply

步驟8.在Settings索引標籤下,導覽至RADIUS Attributes > Standard。按一下Add以新增新屬性 Service-Type。從下拉選單中,選擇Administrative,以提供對對映到此策略的使用者的完全訪問許 可權。按一下「Apply」以儲存變更,如下圖所示。

tings:		
ADIUS Attributes	Attribute Information	andard attribute, and
Standard	áttrík 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	

附註:如果要為特定使用者提供只讀訪問許可權,請從下拉選單中選擇NAS-Prompt。在本示 例中,建立了名為Cisco WLC RO的另一個策略,以便在Domain Users對象名稱下為使用者 提供只讀訪問許可權。

	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							
Overview Conditions Constr	sints 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 andard attribute, and						
Vendor Specific	Attribute name: Service-Type						
Network Access Protection	Attribute ou mber						
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						
TP Filters	(none>						
Encryption	O Commonly used for 802.1x						
R IP Settings	(none>						
	Others						
	NAS Prompt						
	OK Cancel						
	OK Cancel Arr	xly					

驗證

1.使用loginuser憑據時,不允許使用者配置控制器上的任何更改。



General	Security	QoS	Policy-Mapping	Advanced		
Profile Na	ame	tes	tr			
Туре		WL	AN			
SSID		test2				
Status	Status		Enabled			
Security	Policies	F1				inges.)
Radio Po	licy	Autho	rization Failed. No su	fficient privileges		
Interface	/Interface Grou					
Multicast	Vlan Feature				Close	
Broadcas	t SSID	0	Lilavicu			
NAS-ID		nor	ne			

從**debug aaa all enable**中,您可以看到授權響應中的service-type屬性的值為7,該值對應於NASprompt。

```
*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-
*radiusTransportThread: Dec 07 22:20:14.668: AVP[02]
Class.....DATA (44 bytes)
```

```
2.使用adminuser憑據時,使用者應具有與administrative對應的service-type value 6的完全訪問許可
權。
```



*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)

疑難排解

若要對透過NPS對WLC的管理存取進行排解疑難,請執行debug aaa all enable指令。

1.此處顯示了使用不正確憑證時的日誌。

```
*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
*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 e4
....7.....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 Access-Reject received from
RADIUS server 10.106.33.39 (qid:0) with port:1812, pktId:15
```

2.將service-type與Administrative(value=6)或NAS-prompt(value=7)以外的值一起使用時的日誌顯示 如下。在這種情況下,即使身份驗證成功,登入也會失敗。

```
*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:
(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.....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
```