Microsoft NPSによるAireOS WLCの管理アクセス

内容

<u>概要</u>
<u>前提条件</u>
<u>要件</u>
<u>使用するコンポーネント</u>
<u>背景説明</u>
<u>設定</u>
<u>WLC の設定</u>
<u>Microsoft NPSの構成</u>
<u>確認</u>
トラブルシュート

概要

このドキュメントでは、Microsoft Network Policy Server(NPS)を使用してAireOS WLC GUIおよびCLIの管理アクセスを設定する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- ・ワイヤレスセキュリティソリューションに関する知識
- AAAおよびRADIUSの概念
- ・Microsoft Server 2012の基礎知識
- Microsoft NPSおよびActive Directory(AD)のインストール

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアおよびハードウェアコンポーネントに基づいてい ます。

- 8.8.120.0のAireOSコントローラ(5520)
- Microsoft Server 2012

注:このドキュメントは、WLC管理アクセスにMicrosoftサーバで必要な設定例を読者に示 すことを目的としています。このドキュメントで示す Microsoft Windows サーバの設定はラ ボでテスト済みで、期待通りに動作することが確認されています。設定で問題が発生した場 合は、Microsoft に支援を求めてください。Cisco Technical Assistance Center(TAC)は、 Microsoft Windowsサーバの設定をサポートしていません。Microsoft Windows 2012 のイン ストール ガイドと設定ガイドは Microsoft Tech Net にあります。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド キュメントで使用するすべてのデバイスは、初期(デフォルト)設定の状態から起動しています 。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的 な影響について確実に理解しておく必要があります。

背景説明

WLC CLI/GUIにアクセスすると、ユーザはログインに成功するためのクレデンシャルの入力を求められます。クレデンシャルは、ローカルデータベースまたは外部AAAサーバに対して確認できます。このドキュメントでは、外部認証サーバとしてMicrosoft NPSを使用しています。

設定

この例では、AAA(NPS)vizに2人のユーザが設定されています。loginuserとadminuserです。 loginuserは読み取り専用アクセスを持ち、adminuserはフルアクセス権を付与されています。

WLC の設定

ステップ1:コントローラにRADIUSサーバを追加します。[Security] > [RADIUS] > [Authentication]に移動します。[新規]をクリックして、サーバを追加します。次の図に示すように 、このサーバを管理アクセスに使用できるように、管理オプションが有効になっていることを確 認します。

cisco	MONITOR	<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 Local EAP Advanced EAP Priority Order Certificate 	Server In Server Ad Shared Se Shared Se Confirm S Key Wrap Apply Cise Apply Cise Port Num Server St Support f Server Tie Network 1 Managem	dex ddress(Ipv4 ecret Forma ecret Shared Secr co ISE Defa co ACA Def ber atus for CoA meout User sent	//Ipv6) at ret ault settings ault settings	2 10.106.33.35 ASCII © (Designed fo 1812 Enabled © 5 secon ✓ Enable	e FIPS custome	ers and requires a k	ey wrap complia	nt RADIU	S server;
Access Control Lists	Managem	ent Retrans	smit Timeout	5 second	s				
Wireless Protection Policies	Tunnel Pr	оку		Enable					
▶ Web Auth	Realm Lis	8		C Fachla					
TrustSec	TPEac	isioning		Enable					
Local Policies Umbrella	Cisco ACA			Enable					

Advanced

ステップ2:[Security] > [**Priority Order] > [Management User]に移動します**。認証タイプの1つとし てRADIUSが選択されていることを確認します。

MONITOR	<u>W</u> LANs	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT
Priority O	rder > N	lanagement l	Jser		
Authentic	ation				
Not U	Jsed		Order U	sed for Authe	ntication
TACACS	5+	>		RADIUS	Up
		<		Louis	Down

注:認証順序でRADIUSが最初の優先順位として選択されている場合、ローカルクレデンシャルはRADIUSサーバに到達できない場合にのみ認証に使用されます。RADIUSが2番目の 優先順位として選択されている場合、RADIUSクレデンシャルは最初にローカルデータベー スに対して確認され、次に設定済みのRADIUSサーバに対して確認されます。

Microsoft NPSの構成

ステップ1: Microsoft NPSサーバーを開きます。[Radius Clients]を右クリック**します**。[**New**]をクリックして、WLCをRADIUSクライアントとして追加します。

必要な詳細を入力します。RADIUSサーバの追加時に、コントローラに設定されている共有秘密 と同じであることを確認してください。

0	WLC Properties	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: Image: WLC Image: Enable this RADIUS client Address (IP or DNS): Image: Enable this RADIUS client Shared Secret Select an existing Shared Secrets template: None Image: Im	
< III >	OK Cancel Apply	

ステップ2:[Policies] > [**Connection Request Policies]に移動します**。右クリックして新しいポリシ ーを追加します(図を参照)。

•	Cisco WLC Properties	^
File Action View Help File Action View Help Provide the second	Overview Conditions Settings Policy name: Cisco WLC Policy State Fenabled, NPS evaluates this policy while processing connection requests. If disabled, NPS does not evalue this policy. Image: Policy enabled Policy enabled	
Connection Request Po Network Policies Health Policies Network Access Protection System Health Validato Accounting Templates Management	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: 10 0	
К Ш >	OK Cancel Ap	ply

ステップ3:[**Conditions**]タブ**で、**新しい条件として[NAS Identifier]を選択します。プロンプトが表 示されたら、図に示すように、コントローラのホスト名を値として入力します。

	Cisco WLC Properties	x
Overview Conditions Set	lings	
Configure the conditions for If conditions match the conr connection request, NPS s	this network policy. nection request, NPS uses this policy to authorize the connection request. If conditions do not match the rips this policy and evaluates other policies, if additional policies are configured.	
Condition	Value	ן ר
NAS Identifier	Cisco-WLC	
Condition description: The NAS Identifier condition	n specifies a character string that is the name of the network access server (NAS). You can use pattern matching	
Synak to specify the name	Add Edit Remove	
	OK Cancel App	ły

ステップ4:[Policies] > [**Network Policies]に移動します**。右クリックして新しいポリシーを追加し ます。この例では、ポリシーの名前は**Cisco WLC RW**です。これは、ポリシーがフル(読み取り /書き込み)アクセスを提供するために使用されていることを意味します。ポリシーが次のように 設定されていることを確認します。

0	Cisco WLC RW Properties	X
File Action View Help	Overview Conditions Constraints Settings Policy name: Disco WLC RW	
A Control Clients and Servers A RADIUS Clients Remote RADIUS Server A Policies	Policy State If enabled, NPS evaluates this policy while performing authorization. If disabled, NPS does not evaluate this policy. Policy enabled	
Connection Request Po Network Policies Health Policies Network Access Protection	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?	
 Templates Management 	 Grant access. Grant access if the connection request matches this policy. Deny access. Deny access if the connection request matches this policy. Ignore user account dial-in properties. If the connection request matches the conditions and 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. 	
	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.	
	Unspecified v O Vendor specific:	
< III >	OK Cancel Appl	y

ステップ5:[**Conditions**]タブで**[Add**]をクリッ**クします**。図に示すように、[User groups]を選択し、 [Add]をクリックします。

				Cisc	o WLC I	RW Prop	erties					L
Overview	Conditions	Constraints	Settings									
Configure	the condition	ns for this netw	vork policy									
If condition connection	ns match the n request, N	connection r PS skips this p	equest, NP policy and (S uses this p evaluates oth	olicy to aut ner policies,	horize the c if additional	onnection policies	n request. If c are configured	onditio d.	ns do not m	atch the	
					Select	conditio	n					x
Select a	condition, a	and then click	Add.									
Group	s											^
	Windows The Windo groups. Machine (The Machine	Groups ws Groups o Groups ne Groups co	ondition sp andition sp	ecifies that t	the connect	ting user or	er must t	er must belor belong to one	ng to or of the	ne of the se selected g	elected roups.	Ξ
SEA HCAP	User Grou The User (ips Broups condit	tion specif	ies that the c	connecting	user must l	belong to	one of the se	elected	groups.		
	Location (The HCAP required to network ac	Groups Location Gro match this p cess servers	oups condi olicy. The (NASs). S	tion specifies HCAP protoc See your NAS	s the Host col is used S documen	Credential for commu tation befor	Authoriza nication e using t	tion Protoco between NPS his condition	I (HCA S and s	P) location ome third p	groups party	~
									[Add	Can	cel
								Add		Edit	Ren	nove

ステップ6:表示されたダイアロ**グボックス**の[Add Groups]をクリックします。表示される[グル ー**プの選**択]ウィンドウで、目的のオブジェク**トの種類と場所を**選択し**、図に示す**ように、必要な オブジェクト名を入力します。

	Cisco WLC RW Properties	>
Ov	User Groups 🗶	
C If	Specify the group membership required to match this policy. on request. If conditions do not match the	
Å	Groups are configured.	x
		^
		~
		Ξ
	iter must belong to one of the selected	
	Add Groups Remove : belong to one of the selected groups.	
	OK Cancel to one of the selected groups.	
	Select Group	
	Select this object type: pcol (HCAP) location groups	
	Group Object Types VPS and some third party tion.	
	From this location:	~
	wlanlsc.com Locations Add Cancel	
	Enter the object name to select (examples):	
	Domain Admins Check Names	
	Edit Remove	
	Advanced OK Cancel	

条件が正しく追加されると、次のようになります。

			Cisco WLC RW Properties
verview	Conditions	Constraints	Settings
Configure If condition	the condition ons match the on request, N	o connection r PS skips this p	vork 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	ar Groups	W	/LANLSC\Domain Admins
Condition The User	description: Groups cond	lition specifies	s that the connecting user must belong to one of the selected groups.
Condition The User	description: Groups cond	lition specifies	s that the connecting user must belong to one of the selected groups. Add Edt Remove

注:場所とオブジェクト名の詳細を確認するには、active directoryを開き、目的のユーザ名 を探します。この例では、Domain Adminsはフルアクセス権を付与されたユーザーで構成さ れています。adminuserはこのオブジェクト名の一部です。

	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 ar	nd Compute	rs	
File Action View Help		Admin Us	ser Prop	erties	?	x
Active Directory Users and Active Directory Users and Saved Queries 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 ironment	COM- Organizat Sessions	ion ir a rot rot rot rot rot rot rot rot rot rot
	Primary group: 1	Domain Admins There is n you have application	io need to o Macintosh ns.	change Primary clients or POSI)	group unless K-compliant	ist ro ro

ステップ7:[Constraints]タブの下**で**、[Authentication Methods]に移動し、[unencrypted authentication]だけがオンになっている**ことを確認**します。

Cisco WLC RW Properties
Cisco WLC RW Properties X 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 Authentication Methods Allow access only to those clients that authenticate with the specified methods. Image: Authentication Methods EAP types are negotiated between NPS and the client in the order in which they are listed. EAP types EAP types: Image: Called Station ID Move Up Image: NAS Port Type 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 Encrypted authentication (MS-CHAP) User can change password after it has expired Encrypted authentication (CHAP) Vinencrypted authentication (PAP, SPAP) Allow clients to connect without negotiating an authentication method Perform machine health check only OK Cancel

ステップ8:[Settings]タブ**で**、[RADIUS Attributes] > [Standard]に移動します。[追加]をクリックし て、新しい属性Service-Typeを追加します。このポリシーにマップされているユーザーへの完全 なアクセスを提供するには、ドロップダウンメニューから[管理]を選択します。図に示すように、 [Apply]をクリックして変更を保存します。

Standard	Attribute Information	andard attribute, and
Standard		
Vander Cossifie	Attribute name:	ADIUS clients. See
vendor Specific	Service-Type	
letwork Access Protection	Attribute number:	
NAP Enforcement	6	
Kate State	Attribute format:	
Routing and Remote Acc	Enumerator	
Multilink and Bandwid Allocation Protocol (B	Attribute Value: O Commonly used for Dial-Up or VPN	
P IP Filters	(none> V	
Encryption	O Commonly used for 802.1x	
P Settings	<pre></pre>	
	Others	
	Administrative	
	OK Cancel	

注:特定のユーザに対して読み取り専用アクセスを許可する場合は、ドロップダウンから [NAS-Prompt]を選択します。この例では、[Domain Users]オブジェクト名の下のユーザに読 み取り専用アクセスを提供するために、Cisco WLC ROという名前の別のポリシーが作成さ れます。

	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 Constr	aints Settings	
Configure the settings for this r If conditions and constraints m	etwork policy. atch the connection request and the policy grants access, settings are applied.	
Settings:		_
RADIUS Attributes	Attribute Information	
Vendor Specific	Attribute name: Service-Type	
Network Access Protection	Attribute number:	
NAP Enforcement	6	
p Extended State	Attribute format:	
Routing and Remote Acc	chumerator	
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 V	
	OK Cancel	
	OK Cancel Ap	ply

確認

1.ログインユー**ザー**資格情報を使用する場合、ユーザーはコントローラーに変更を構成できませ ん。



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

debug aaa all enableから、許可応答のservice-type属性の値が7(NASプロンプトに対応)である ことがわかります。

```
*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.管理者ユーザーの資格情報を使用する場合、ユーザーは管理に対応するservice-type値6を使用
して完全にアクセスする必要があります。
```



```
*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:01:00:00:00:00 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.....0x0000001
*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)
```

トラブルシュート

NPSを介したWLCへの管理アクセスをトラブルシューティングするには、**debug aaa all enableコ マンドを実行**します。

1.誤ったクレデンシャルが使用された場合のログを次に示します。

*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 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-typeがAdministrative (value=6)またはNAS-prompt (value=7)以外の値で使用される場合のログを次に示します。この場合、認証が成功してもログインは失敗します。

*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-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