使用GUI進行登入身份驗證的Aironet接入點上的 TACACS+配置示例

目錄

 箇介

 必要條件

 需求

 採用元件

 慣例

 設定

 網路圖表

 配置TACACS+伺服器進行登入身份驗證 — 使用ACS 4.1

 配置TACACS+伺服器進行登入身份驗證 — 使用ACS 5.2

 為TACACS+身份驗證配置Aironet AP

 驗證

 ACS 5.2驗證

 疑難排解

 相關資訊

<u>簡介</u>

本檔案將說明如何在Cisco Aironet存取點(AP)上啟用TACACS Plus(TACACS+)服務,以便使用 TACACS+伺服器執行登入驗證。

<u>必要條件</u>

<u>需求</u>

嘗試此組態之前,請確保符合以下要求:

- 瞭解如何在Aironet AP上配置基本引數
- •瞭解如何配置TACACS+伺服器(如思科安全訪問控制伺服器(ACS))的知識
- TACACS+概念知識

有關TACACS+如何工作的資訊,請參閱<u>設定RADIUS和TACACS+伺服器的瞭解TACACS+</u>一節。

<u>採用元件</u>

本文中的資訊係根據以下軟體和硬體版本:

• Aironet Cisco Aironet 1240/1140系列存取點

- 運行軟體版本4.1的ACS
- 運行軟體版本5.2的ACS

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。

<u>慣例</u>

如需文件慣例的詳細資訊,請參閱思科技術提示慣例。

<u>設定</u>

本節介紹如何將Aironet AP和TACACS+伺服器(ACS)配置為基於TACACS+的登入身份驗證。

此配置示例使用以下引數:

- ACS的IP地址 172.16.1.1/255.255.0.0
- AP的IP地址 172.16.1.30/255.255.0.0
- AP和TACACS+伺服器上使用的共用金鑰 示例

以下是此示例在ACS上配置的使用者的憑據:

- 使用者名稱- User1
- •密碼—Cisco
- 組 AdminUsers

您需要配置TACACS+功能,以驗證嘗試通過Web介面或通過命令列介面(CLI)連線到AP的使用者。 為了完成此配置,您必須執行以下任務:

- 1. <u>配置TACACS+伺服器進行登入身份驗證</u>。
- 2. <u>為Aironet AP配置TACACS+身份驗證</u>。
- 註:使用<u>Command Lookup Tool</u>(僅限<u>註冊</u>客戶)查詢有關本文檔中使用的命令的更多資訊。

網路圖表

本檔案會使用以下網路設定:



配置TACACS+伺服器進行登入身份驗證 — 使用ACS 4.1

第一步是設定TACACS+後台程式,以驗證嘗試訪問AP的使用者。必須設定ACS進行TACACS+身 份驗證並建立使用者資料庫。您可以使用任何TACACS+伺服器。此示例使用ACS作為TACACS+伺 服器。請完成以下步驟: 1. 完成以下步驟,以便將AP新增為身份驗證、授權和記帳(AAA)客戶端:在ACS GUI中,按一下 Network Configuration頁籤。在AAA Clients下,按一下Add Entry。在「新增AAA客戶端」視 窗中,輸入AP主機名、AP的IP地址和共用金鑰。此共用金鑰必須與您在AP上配置的共用金鑰 相同。在「Authenticate Using」下拉選單中,選擇TACACS+(Cisco IOS)。按一下「Submit + Restart」以儲存組態。以下是範例

:

:

CiscoSecure ACS - N	Microsoft Internet Explorer	
Elle Edit View Fg	varkes Iools tjelp	Leis » 🏦
Address Altp://127.0	0.0.1:1065/	- C - C - C - C - C - C - C - C - C - C
Casco Statems	Network Configuration	×
Liter Setup	Add AAA Client	Help Add Client Hestnesse
Brang Stop Shared Profile Components Network Configuration Configuration	AAA Client Hostname AccessPoint AAA Client IP Address Shared Secret Example	AAA Client IP Address Shared Secret Nativerk Device Genue PAD205 Key Write Anthenticate Using Single General: TACACS + AAA Client Leg Medite/WriteMole Packets from this AAA Client Leg SAD205 Instelling Packets from this AAA Client
Administration Configuration Control Control	RADIUS Key Wrap Key Encryption Key Message Authenticator Code Key	Replace Solids: Part with well Usersame from the AAA Clean Statch framed IP. Address with user IP. address for accounting packets from this AAA clean
Papture Validation	Authenticate Using TACACS+ (Cisco IOS)	AAA Client Hestname The AAA Client Histname is the name assigned to the AAA client.
Reports and Activity	Single Connect TACACS+ AAA Client (Record stop in accounting on failure) Log Update/Watchdog Packets from this AAA Client	Ratk to Tep
Contraction Documentation	Log RADIUS Tunneling Packets from this AAA Client Replace RADIUS Port info with Username from this AAA Client	The AAA Client IP Address is the IP address assigned to the AAA client.
	Match Framed-IP-Address with user IP address for accounting packets from this AAA Client Submit Submit + Apply Cancel	If you want to designate more than one AAA client with a single AAA client entry in ACS, you can spacify the IP address for each AAA client to be represented by this AAA client entry. To separate each IP address, press Enter.
	🗖 an ann an an an ann an ann an ann an agus ann an agus ann an an a' ann a' bhail ann an	The second secon

此示例使用:AAA客戶端主機名AccessPoint地址172.16.1.30/16作為AAA客戶端IP地址共用金 鑰示**例**

2. 完成以下步驟,建立包含所有管理(admin)使用者的組:從左側選單中按一下Group Setup。出現一個新視窗。在「組設定」視窗中,從下拉選單中選擇要配置的組,然後按一下重新命名組。此示例從下拉選單中選擇組6,並將該組重新命名為AdminUsers。按一下「Submit」。以下是範例

CiscoSecure ACS - 1	Microsoft Internet Explorer	. (#) ×
Ele Edt yew Fg	vorites Iools Help	Leás 🍅 🍂
Agdress Antp://127.	0.0.1:1965/	• 🔂 🐼
Cinco Sverens	Group Setup	×
	Select	Help
Setup	Renaming Group: Group 6	Rename Gross
Bell Setup		
SharedProfile Components	Group AdminUsers	Rename Group
Network Configuration	Submit Cancel	Type a new group name and click Submit to assign a more description name to the group profile. This is useful if different groups have been configured to allow specific artherization privileges, such
Sustem Configuration		as PPP or Telnet-only capability.
Interface Configuration	😤 Elack to Herb	Click Cancel to return to the Group Setup window without saving a new group name.
Administration Control		[Back to Teal
Di External User Dutabases		
Posture Validation		
Network Access Profiles		
Reports and Activity		
Deline Decomentation		
19		i Internet

3. 完成以下步驟,即可將使用者新增到TACACS+資料庫:按一下**User Setup**頁籤。若要建立新 使用者,請在「使用者」欄位中輸入使用者名稱,然後按一下**新增/編輯**。以下是建立**User**1的 **示例**

:



按一下「新增/編輯」後,將出現此使用者的「新增/編輯」視窗。

:

 输入此使用者特定的憑據,然後按一下Submit以儲存配置。您可以輸入的憑證包括:補充使用 者資訊使用者設定使用者分配到的組以下是範例

File File Manuel	arefuse Tools Malo	1111 - 39 - Age
Address http:///27.0	onces Loos Beb	ມກຣ ~ 🙀 ອີໂດ
Ener Energy	Llees Cature	
	User Setup	
- effilies effilies	Edit	A Help
User Setup	Llear Llear1 (Naw Llear)	Account Displied
Group	User: User1 (New User)	Defeting a Username Supplies a Username
an I Shared Draffin	C Account Disabled	Passweed Authentication
Components		Galback
Network Configuration	Supplementary User Info 🕺	Chent IP Address Assignment Advanced Settings
Sustem Configuration	Real Name User1	Network Access Restrictions Max Sessions
Interface	Description	Usage Oustas Account Disable
Configuration		Opymiaadable.ACLs Advanced TACACS+ Settings
Administration Centrel		TACALS+ Enable Control TACALS+ Enable Passment
Dutabases	User Setup 🤶	TACACS + Outbound Passment TACACS + Shell Command Authorization
Perfure Validation	Password Authentication:	Command Authorization for Network Device Management Applications TACACS + Unknown Services
SelNetwork Access	ACS Internal Database	IETF RADIUS Attributes RADIUS Yender Specific Attributes
Profiles	CHAP/ARAP, if the Separate field is not	
Reports and Activity	Checked.)	
Online Documentation	Confirm	Account Disabled Status
	Password	the check box to enable the account.
	Separate (CHAP/MS-CHAP/ARAP) Dessword	[Back to Tap]
	Confirm	Deleting a Username
	Password	The Delete button appears only when you are editing an existing user account not when you are adding a new user account. To delete the
	cumplying a constant CHAD paceword for a token	current user account from the database, click Delete. When asked to confirm your action, click OK.
	Submit Cancel	(Back to Tan)
8] //		😴 Internet
您可以看到.	比示例將使用者User1新增到組AdminU	sers。
File Edit Yew Fa	vortes Tools Help	Links ** 👔
Address a http://127.	3.0.1:1065/	۰ 🛃 د
Custo Starbud	User Setun	X
db_db_		
	5	
User	User Setup 🌹	≏_ Help
Setup	User Setup	the second Disabled
Group Setup	User Setup ? Password Authentication: ACS Internal Database	Belp Accesst Disabled Ording a Unormane Supplementary User Infe
Group Setup	User Setup Password Authentication: ACS Internal Database CiscoSecure PAP (Also used for CHAP/MS-	Account Disabled Ordering a Unormann Supplementary Unor Info Caserroot Anthentication Croup to twick the user is assigned
Setup Setup Setup Components	User Setup Password Authentication: ACS Internal Database CiscoSecure PAP (Also used for CHAP/MS- CHAP/ARAP, if the Separate field is not checked.)	Account Disabled Account Disabled Account and the second of
Setup Setup Shared Profile Components Retriark Configuration	User Setup Password Authentication: ACS Internal Database CiscoSecure PAP (Also used for CHAP/MS- CHAP/ARAP, if the Separate field is not checked.) Password	Belp Account Disabled Belixing a Unername Supplementary Uner Infe Eassment Artikentication Crange to relick then user is assigned Callback Signat IP Address Assignment Advanced Settleme Network Access Restrictions
Setup Croup Shared Profile Components Net vork Configuration System Configuration	User Setup Password Authentication: ACS Internal Database CiscoSecure PAP (Also used for CHAP/MS- CHAP/ARAP, if the Separate field is not checked.) Password Confirm Password	Account Disabled Callback Callback Callback Callback Advanced Settlines Network Access Restrictions Hat Constant Man Constant
Setup Se	User Setup Password Authentication: ACS Internal Database CiscoSecure PAP (Also used for CHAP/MS- CHAP/ARAP, if the Separate field is not checked.) Password Confirm Password Separate (CHAP/MS-CHAP/ARAP)	Accessit Disabled Accessit Quarking Accessit Quarking Accessit Quarking Authentication Campoint and Quarking Callback Cantored Callback Callback Cantored Callback Callback Callback Callback Cantored Callback Callback Cantored Callback
Setup Stared Profile Components Net-ourisk Configuration System Configuration Interface Configuration	User Setup Password Authentication: ACS Internal Database CiscoSecure PAP (Also used for CHAP/MS- CHAP/ARAP, if the Separate field is not checked.) Password Confirm Password Separate (CHAP/MS-CHAP/ARAP) Password	Account Disabled Account Disable Account Disabl
Setup Setup Setup Setup Setup Configuration Configuration Configuration Configuration Configuration Configuration	User Setup Password Authentication: ACS Internal Database CiscoSecure PAP (Also used for CHAP/MS-CHAP/ARAP, if the Separate field is not checked.) Password Confirm Password Separate (CHAP/MS-CHAP/ARAP) Password Confirm Password	Account Disabled Account Disabled Account Disabled Deleting a Usersame Surplementary User Infe Passesoid Authentication Corps to which the user is assigned Callent IP Address Assignment Advanced Settings Value Sectore Assignment Advanced Settings User Device Assignment Advanced Factore TacActs - Earther Control TaCActs - Earther Descended TaCActs - Control TacActs - Control TacActs - Control
Setup Se	User Setup Password Authentication: ACS Internal Database CiscoSecure PAP (Also used for CHAP/MS- CHAP/ARAP, if the Separate field is not checked.) Password Confirm Password Separate (CHAP/MS-CHAP/ARAP) Password Confirm Password When a token server is used for authentication,	Accessit Disabled Accessit Disabled Deficting a Unername Supplementary Uner Lafe Supplementary Uner Lafe Cathook Cathook
Setup Setup Shared Profile Components Net vark Configuration System Configuration System Configuration Methods Configuration Setup Interface Configuration Setup Interface Configuration Setup Partice Partice Partice Partice Partice	User Setup Password Authentication: ACS Internal Database CiscoSecure PAP (Also used for CHAP/MS- CHAP/ARAP, if the Separate field is not checked.) Password Confirm Password Separate (CHAP/MS-CHAP/ARAP) Password Confirm Password When a token server is used for authentication, supplying a separate CHAP password for a token card user allows CHAP authentication. This is	Account Disabled Callack Callack Callack Callack Callack Callack Advanced Settings Network Access Restrictions Han Sestion Access Disable Access
Setup Se	User Setup Password Authentication: ACS Internal Database CiscoSecure PAP (Also used for CHAP/MS- CHAP/ARAP, if the Separate field is not checked.) Password Confirm Password Separate (CHAP/MS-CHAP/ARAP) Password Confirm Password When a token server is used for authentication, supplying a separate CHAP password for a token card user allows CHAP authentication. This is especially useful when token caching is enabled.	Account Divabled Account Divabled Account Structure Account Structure Authentication Compt to which the user is assigned Callback Client IP Address Assignment Advanced Settings Advanced Settings Vistore Access Restrictions Man Sessions Vistore Access Restrictions Advanced Settings Vistore Overlas Advanced Settings Vistore Overlas Advanced TACACS - Settings IdeAccess Tacking IdeAccess Control IACACS - Enable Control IACACS - Conthermond Authorization Command Authorization Kernel Settings IACACS - Maniferment Settings
Setup Se	User Setup Password Authentication: ACS Internal Database CiscoSecure PAP (Also used for CHAP/MS- CHAP/ARAP, if the Separate field is not checked.) Password Oonfirm Password Separate (CHAP/MS-CHAP/ARAP) Password Confirm Password When a token server is used for authentication, supplying a separate CHAP password for a token card user allows CHAP authentication. This is especially useful when token caching is enabled. Group to which the user is assigned:	Accent Divalied Accent Divalies Accent Divalie A
Setup Setup Shared Profile Components System Configuration System Configuration Metwork Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration System Configuration Configuration System Configuration Configuration Configuration System Configuration Configuration Configuration System Configuration Configuration Configuration System Configuration Configuration Configuration System Configuration Configuration System Configuration Con	User Setup Password Authentication: ACS Internal Database CiscoSecure PAP (Also used for CHAP/MS- CHAP/ARAP, if the Separate field is not checked.) Password Password Separate (CHAP/MS-CHAP/ARAP) Password Confirm Password Confirm Password When a token server is used for authentication, supplying a separate CHAP password for a token card user allows CHAP authentication. This is especially useful when token caching is enabled. Group to which the user is assigned: AdminUsers	Account Disabled Account Disabled Account Disabled Account Disabled Action of the series and the series of
Setup Se	User Setup Password Authentication: ACS Internal Database CiscoSecure PAP (Also used for CHAP/MS-CHAP/ARAP, if the Separate field is not checked.) Password Confirm Password Separate (CHAP/MS-CHAP/ARAP) Password Confirm Password When a token server is used for authentication, supplying a separate CHAP password for a token card user allows CHAP authentication. This is especially useful when token caching is enabled. Group to which the user is assigned: Callback	Account Divabled Account Divabled Account Divabled Account Divabled Account Divabled Authoritation Campa Development Campa Development Cathood Ca
Setup Se		Access Disabled Access

■ Callback using this number
註:如果未建立特定組,則使用者將被分配到預設組。

5. 完成以下步驟以定義許可權級別:按一下Group Setup選項卡。選擇之前分配給此使用者的組

,然後按一下**編輯設定**。此示例使用組AdminUsers。在TACACS+設定下,選中**Shell(exec)**覈 取方塊,並選中值為15的**Privilege level**覈取方塊。按一下「**Submit + Restart**」。

the fifth Many Fo	microsoft internet Exporer	
de Los year rg	V 0 1-10/2) Juones Tone Geb	
fund farmer	Crown Colum	
	Group Setup	
ad bad ba	Jacob Access Restrictions	Help
User Setup Setup Setup Setup Setup Shared Profile Components Components Readinguration Sector Sector Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration	In access control list Out access control list Route Routing Routing Route Shell (exec) Access control list Auto command Callback line Callback rotary	Group Disabled Yoick source: IP (YOIP) Support Default Time-of-Day Access Settings Callback Network Access Restrictions Man Sestions Usage Quarter Vision Carls Inable Options Taken Carl Settings Password Aging Roles Ip Assignment Deventsadable ACLs TACACS - Settings TA
Validation Validation Network Access Profiles Reports and Activity Online Documentation	□ Idle time	 To enable administrators to tailor what authorizations are displayed for a configuration and to simplify the interface, ACS displays only the information options and security protocal attributes are displayed in Group Setup only in the following circumstances: A AAA dient that uses the specified protocol has been configured in the Network Configuration section. For example, RADIUS settings appear only if you have configured a AAA dient that uses RADIUS. The specific services, protocols, and attributes have been selected for display for the appropriate protocol in the Interface Configuration section. A Token Card Server has been configured in the External User Databases section.

註意:必須為GUI和Telnet定義許可權級別15才能作為級別15訪問。否則,預設情況下,使用 者只能作為級別1訪問。如果未定義許可權級別,且使用者嘗試在CLI上進入啟用模式(使用 Telnet),AP將顯示以下錯誤消息:

AccessPoint>**enable**

% Error in authentication

如果要向TACACS+資料庫新增更多使用者,請重複此過程中的步驟2到步驟4。完成這些步驟後 ,TACACS+伺服器即可驗證嘗試登入到AP的使用者。現在,您必須為TACACS+身份驗證配置 AP。

配置TACACS+伺服器進行登入身份驗證 — 使用ACS 5.2

第一步是在ACS中將AP新增為AAA客戶端,並為登入建立TACACS策略。

1. 完成以下步驟,以便將AP新增為AAA客戶端:在ACS GUI中,按一下Network Resources,然後按一下Network Devices and AAA Clients。在Network Devices下,按一下Create。在名稱中輸入AP的主機名,並提供有關AP的說明。如果定義了這些類別,請選擇Location和Device Type。由於只配置單個AP,請按一下單個IP地址。您可以通過按一下IP Range(s)新增多個 AP的IP地址範圍。然後,輸入AP的IP地址。在Authentication Options下,選中TACACS+框,並輸入Shared Secret。以下是範例

* 🚭 My Workspace	Network Resources > Network Devices and AAA Climits > Crede			de la companya
All Metwork Personnes Network Device Groups Location Device Type Type	Name AP1160 Description: Autonomous AP1140 of Foor 1 Network Device Groups Description: Descriptio			
Default Network Device External RADIUS Servers	Device Type All Device Types	Select		
Overs and identity literes Oversets Oversets Access Policies Monitoring and Reports Overset Administration	P Address * Single P Address C. IF Range(s) • P. 17210130		Authentication Options	

2. 下一步是建立登入使用者名稱和密碼:按一下Users and Identity Stores,然後按一下Users。 按一下「Create」。在Name下提供使用者名稱,並提供說明。選擇身份組(如果有)。在 Password文本框中輸入密碼,然後在Confirm Password下重新輸入。您可以在Enable Password下輸入密碼,以修改啟用密碼。重新輸入以確認。以下是範例

• Melecok Resources • Melecok Resources • Melecok Resources • Meterial Identify Oncups • Oncuts • Identify Oncups • Oncuts • Identify Oncups • Oncuts • Oncuts <t< th=""><th> MyWorkspace </th><th>Users and identify Stores + Internal identity Stores</th><th>- Users - Create</th><th></th><th></th><th></th><th></th><th></th></t<>	 MyWorkspace 	Users and identify Stores + Internal identity Stores	- Users - Create					
	Control of the second sec	General Name csec123 Description: Login for Autonomous Description: All Groups Password Information Password must Contian 4 - 32 characters Password must Continn Password enmet login Change password en met login User Information There are no additional identity attribute C Password States	Status: Enable AP	d • •	Dable Password Int Password must • Contain 4 - 32 Enable Password Quefins Password	formation 2 chanacters *******		

3. 完成以下步驟以定義許可權級別:按一下Policy Elements > Authorizations and Permissions > Device Administration > Shell Profiles。選中Permit Access覈取方塊,然後按一下Duplicate。



輸入**名稱**和說明。



選擇Common Tasks頁籤,然後選擇15作為最大許可權。

CALIFY COMPANY AND A COMPANY AND A COMPANY	Policy Benerits × Authorization and Penessions × Device Administration × Shell Profiles × Duplicate. "Penel Access"
Ut Network Resources	
a Users and Identity Stores	Ceneral Common Tasks Custom Athlutes
C. Dates Dements	Protinge Level
Session Conditions	Defaul Privilege: Not in Use -
Date and Time	Maximum Privlege Etate • Value 15 •
Custom	Shell Attributes
 Network Conditions Automatication 	Access Control List Notin Use - 2
 Network Access 	Add Command Natio Use -
Device Administration	In Consider A March 19
Stell Profes	
Command Sets	Ne Escape Notin Use - a
C - Arress Policies	No Hang Up: Notin Use - 10
B Muniferen and Banada	Timeout Natim Use - 11
monitoring and methods	Kite Time Notin Use - 12
Gyslem Administration	Calibration Networks - 14
	Central moder Protection
	• = Required fields

按一下「Submit」。

4. 完成以下步驟以建立授權策略:按一下「Access Policies」>「Access Services」>「Default Device Admin」>「Authorization」。按一下Create以建立新的授權策略。此時會出現一個新

的彈出視窗,用於為授權策略建立規則。選擇特定使用者名稱和AAA客戶端(AP)的**身份組、位** 置等(如果有)。按一下Shell Profile的**Select**以選擇已建立的Autonomous AP的配置檔案。

alah		Cisco Secure ACS - MooRe Firefox	• vamaniace\$2.071may0 LogDd Abod Hep
cisco Cisco Secure A	CS	B. https://25.395.127.39/accodminiPolicy/inpublicition.do.	
Ally Workspace Default Device Administration Ally Workspace Orbust Network Access Montering and Reports System Administration	Access Falce Standard Pro Device Adr Filter, Sta 1	Several None: Adaroomous AP Status: Enabled Image: Status and results are available here for use in policy rules screen controls which policy conditions and results are available here for use in policy rules. Conditions Indentity Orsup: -ANF NDOLuccation: -ANF NDOLuccation: -ANF NDOLuccation: -ANF Image: Antional control of the policy rules -ANF NDOLuccation: -ANF Image: Antional control of the policy rules -ANF Bellett -ANF Bellett -ANF	
	- El Create_1		Customize Hit Count

完成此操作後,按一下Save Changes。按一下Default Device Admin,然後按一下Allowed Protocols。選中Allow PAP/ASCII,然後按一下Submit。按一下Service Selection Rules,確儲存在與TACACS匹配且指向Default Device Admin的規則。

cisco Cisco Secure Ad	CS			er sedmen	represienti (Minery)	LopOut	About 1990
* 😚 MyWaftspace	Access Policies + Access Services + Default Device Admin + Ealt. "Default Device Admin"	SEAS STREET					
Organization Second S	Ceneral Moveed Protocols Process Hold Lookup Automitation Protocols Image: Charped Image: Autom MS-CHArped I					Logical	
Gisco Cisco Secure At Gisco Secure At	Access Fables + Access Service Selection Pules						
10 Network Resources 20 Users and identity Stores	Single result selection P Rule based result selection						
Policy Elements	Filter Status - Match if Equals - Enabled - Clear Filter	00 -		11-14-1-N		055050	
Access Dences Access Dences	Conditions	Results	HECount				
O Default Device Admin Identity	1 2 0 Euler match Tacacs	Default Device Admin Default Network Access	25 0				
O Default Network Access Monitoring and Reports Monitoring and Reports Monitoring and Reports							
	Context If no rules defined or no enabled rule matches.	DenyAccess	0				
	Create_1+ Duplicate_1+ Edit Develo				Custor	nize Hit	Count
	Cave Changes Discard Changes						

為TACACS+身份驗證配置Aironet AP

:

您可以使用CLI或GUI在Aironet AP上啟用TACACS+功能。本節介紹如何使用GUI為TACACS+登入 身份驗證配置AP。

完成以下步驟,以便使用GUI在AP上設定TACACS+:

 完成以下步驟以定義TACACS+伺服器引數:在AP GUI中選擇Security > Server Manager。安全性:出現「Server Manager(伺服器管理器)」視窗。在Corporate Servers區域,從 Current Server List下拉選單中選擇TACACS+。在此相同區域中,輸入TACACS+伺服器的 IP地址、共用金鑰和身份驗證埠號。按一下「Apply」。以下是範例



注意:預設情況下,TACACS+使用TCP埠49。**注意:**您在ACS和AP上配置的共用金鑰必須匹 配。

 2. 選擇Default Server Priorities > Admin Authentication(TACACS+), 從Priority 1下拉選單中選 擇已配置的TACACS+伺服器IP地址,然後按一下Apply。以下是範例

3	Cisco 105 Series AP - Securit	y - Server Manager - Microsoft	Internet Explorer provided by Cisco Sy	stems, Inc.		X
J	Ele Edit Yew Pavorites	Toop Geb				100
J	4=Back + -> -> 🕥 🔁 🖾	Search @Favorites @1	Neda 🎯 🛂 🥥 📾 🖬 🎯 👯			
JA	lgdress 👸 http://10.77.244.194	ijap_sec_network-security_a.shtml#	KorpServers		- 0	Go Links **
Π						-
П						
П		Delete	Authentication Port (optional):	49 (0-65536)		
П			Accounting Port (optional):	DISABLED (0-65536)		
П					Annhy Car	Incel
					-499	
		Default Server Priorities				
П		EAP Authentication	MAC Authentic	ation	Accounting	
		Priority 1: (NONE > .	Priority 1: NO	DNE > •	Priority 1: NONE > •	
		Priority 2: (NONE)	Priority 2: (NC	ONE > ¥	Priority 2: (NONE)	
		Priority 3 (NONE)	Priority 3: KNC	ONE > *	Printy 3: (NONE)	
П		rindy a letter a	r namy s. p		rinning or [
		Admin Authentication (R	ADIUS) Admin Authent	ication (TACACS+)		
		Division (ANONE N	Division 172	1611		
		Priority 1: CNUME 7	Priority 1: 172	10.1.1		
П		Priority 2: (NONE)	Priority 2: KNC	ONE > 💌		
П		Priority 3: < NONE > .	Priority 3: KNC	ONE > 💌		
					Apply Car	icel
ľ						
	Close W	andow			opyright (c) 1992-2006 by Cisco Syst	Jerns, Inc.
D					Dirternet	

3. 選擇**Security > Admin Access**,對於Administrator Authenticated by:,選擇**Authentication Server Only**,然後按一下**Apply**。此選擇可確保嘗試登入到AP的使用者由身份驗證伺服器進行 身份驗證。以下是範例

:



以下是組態範例的CLI組態:

接入點
AccessPoint# show running-config
Current configuration : 2535 bytes
version 12.3
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
hostname AccessPoint
1
: ip_submet-zero
1 ·
!
aaa new-model
<pre>! Enable AAA. ! ! aaa group server radius rad_eap !</pre>
aaa group server radius rad_mac ! aaa group server
radius rad_acct ! aaa group server radius rad_admin
cache expiry 1 cache authorization profile admin_cache
cache authentication profile admin_cache ! aaa group
Configure the server group tac admin. server
172.16.1.1
! Add the TACACS+ server 172.16.1.1 to the server
group. cache expiry 1

Set the expiration time for the local cache as 24 hours. cache authorization profile admin_cache cache authentication profile admin_cache aaa group server radius rad_pmip ! aaa group server radius dummy ! aaa authentication login default group tac_admin !--- Define the AAA login authentication method list to use the TACACS+ server. aaa authentication login eap_methods group rad_eap aaa authentication login mac_methods local aaa authorization exec default group tac admin !--- Use TACACS+ for privileged EXEC access authorization !--- if authentication was performed with use of TACACS+. aaa accounting network acct_methods start-stop group rad_acct aaa cache profile admin_cache all ! aaa session-id common ! ! username Cisco password 7 00271A150754 ! bridge irb ! ! interface Dot11Radio0 no ip address no ip route-cache shutdown speed basic-1.0 basic-2.0 basic-5.5 basic-11.0 station-role root bridgegroup 1 bridge-group 1 subscriber-loop-control bridgegroup 1 block-unknown-source no bridge-group 1 sourcelearning no bridge-group 1 unicast-flooding bridge-group 1 spanning-disabled ! interface Dot11Radio1 no ip address no ip route-cache shutdown speed station-role root bridge-group 1 bridge-group 1 subscriber-loopcontrol bridge-group 1 block-unknown-source no bridgegroup 1 source-learning no bridge-group 1 unicastflooding bridge-group 1 spanning-disabled ! interface FastEthernet0 no ip address no ip route-cache duplex auto speed auto bridge-group 1 no bridge-group 1 sourcelearning bridge-group 1 spanning-disabled ! interface BVI1 ip address 172.16.1.30 255.255.0.0 no ip routecache ! ip http server ip http authentication aaa !--- Specify the authentication method of HTTP users as AAA. no ip http secure-server ip http help-path http://www.cisco.com/warp/public/779/smbiz/prodconfig/he lp/ea ip radius source-interface BVI1 ! tacacs-server host 172.16.1.1 port 49 key 7 13200F13061C082F tacacsserver directed-request radius-server attribute 32 include-in-access-req format %h radius-server vsa send accounting ! control-plane ! bridge 1 route ip ! ! ! line con 0 transport preferred all transport output all line vty 0 4 transport preferred all transport input all transport output all line vty 5 15 transport preferred all transport input all transport output all ! end

注意:您必須使用Cisco IOS軟體版本12.3(7)JA或更新版本,才能使此配置中的所有命令正常運行 。早期的Cisco IOS軟體版本可能沒有這些命令可用。

<u>驗證</u>

使用本節內容,確認您的組態是否正常運作。

<u>輸出直譯器工具</u>(僅供<u>已註冊</u>客戶使用)(OIT)支援某些**show**命令。使用OIT檢視**show**命令輸出的分析 。

若要驗證設定,請嘗試使用GUI或CLI登入AP。當您嘗試訪問AP時,AP會提示您輸入使用者名稱和

密碼。

<mark>Ente</mark> r Netv	vork Passwor	rd 🛛	<u>?</u> ×
? >	Please type yo	our user name and password.	
IJ	Site:	172.16.1.30	
	Realm	level_1_access	
	User Name	User1	
	Password	****	
	🔲 Save this p	password in your password list	
		OK Ca	ancel

提供使用者認證時,AP會將認證轉送到TACACS+伺服器。TACACS+伺服器根據資料庫中提供的 資訊驗證憑證,並在身份驗證成功後提供對AP的訪問。您可以在ACS上選擇**Reports and Activity > Passed Authentication**,並使用Passed Authentication報告檢查此使用者的身份驗證是否成功。以 下是範例:

Select								
🖹 <u>Refresh</u>	Down	load						
Passed Authentications active.csv								
Date	<u>Time</u>	Message- <u>Type</u>	<u>User-</u> <u>Name</u>	<u>Group-</u> <u>Name</u>	Caller-ID	NAS- Port	<u>NAS-IP-</u> <u>Address</u>	
05/10/2006	14:57:01	Authen OK	User1	AdminUsers	172.16.1.1	tty 1	172.16.1.30	

您還可以使用show tacacs命令來驗證TACACS+伺服器的正確配置。以下是範例:

AccessPoint# show	tacacs

Tacacs+ Server :	172.16.1.1/49
Socket opens:	348
Socket closes:	348
Socket aborts:	0
Socket errors:	0
Socket Timeouts:	0
Failed Connect Attempts:	0
Total Packets Sent:	525
Total Packets Recv:	525



您可以驗證來自ACS 5.2的登入憑證失敗/通過嘗試:

- 按一下Monitoring and Reports > Launch Monitoring and Report Viewer。將開啟一個包含儀 表板的新彈出視窗。
- 2. 按一下「Authentications-TACACS-Today」。這顯示失敗/通過嘗試的詳細資訊。

疑難排解

您可以在AP上使用以下debug指令對組態進行疑難排解:

附註:使用 debug 指令之前,請先參閱<u>有關 Debug 指令的重要資訊</u>。

- debug tacacs events 此命令顯示TACACS身份驗證期間發生的事件序列。以下是此指令輸 出的範例: *Mar 1 00:51:21.113: TPLUS: Queuing AAA Authentication request 0 for processing *Mar 1 00:51:21.113: TPLUS: processing authentication start request id 0 *Mar 1 00:51:21.113: TPLUS: Authentication start packet created for 0(User1) *Mar 1 00:51:21.114: TPLUS: Using server 172.16.1.1 *Mar 1 00:51:21.115: TPLUS(0000000)/0/NB_WAIT/C6DC40: Started 5 sec timeout 1 00:51:21.116: TPLUS(0000000)/0/NB_WAIT: socket event 2 *Mar *Mar 1 00:51:21.116: TPLUS(0000000)/0/NB_WAIT: wrote entire 25 bytes request *Mar 1 00:51:21.116: TPLUS(0000000)/0/READ: socket event 1 *Mar 1 00:51:21.117: TPLUS(00000000)/0/READ: Would block while reading *Mar 1 00:51:21.120: TPLUS(00000000)/0/READ: socket event 1 *Mar 1 00:51:21.120: TPLUS(0000000)/0/READ: read entire 12 header bytes (expect 16 bytes data) *Mar 1 00:51:21.120: TPLUS(0000000)/0/READ: socket event 1 *Mar 1 00:51:21.120: TPLUS(0000000)/0/READ: read entire 28 bytes response *Mar 1 00:51:21.121: TPLUS(0000000)/0/C6DC40: Processing the reply packet *Mar 1 00:51:21.121: TPLUS: Received authen response status GET_PASSWORD (8) *Mar 1 00:51:21.121: TPLUS: Queuing AAA Authentication request 0 for processing *Mar 1 00:51:21.121: TPLUS: processing authentication continue request id 0 *Mar 1 00:51:21.122: TPLUS: Authentication continue packet generated for 0 *Mar 1 00:51:21.122: TPLUS(0000000)/0/WRITE/C6DC40: Started 5 sec timeout 1 00:51:21.122: TPLUS(0000000)/0/WRITE: wrote entire 22 bytes request *Mar *Mar 1 00:51:21.178: TPLUS(0000000)/0/READ: socket event 1 *Mar 1 00:51:21.178: TPLUS(00000000)/0/READ: read entire 12 header bytes (expect 6 bytes data) *Mar 1 00:51:21.178: TPLUS(00000000)/0/READ: socket event 1 *Mar 1 00:51:21.178: TPLUS(0000000)/0/READ: read entire 18 bytes response *Mar 1 00:51:21.179: TPLUS(0000000)/0/C6DC40: Processing the reply packet *Mar 1 00:51:21.179: TPLUS: Received authen response status PASS (2)
- debug ip http authentication 使用此命令排除HTTP身份驗證問題。命令顯示路由器嘗試的身份驗證方法和身份驗證特定的狀態消息。

• debug aaa authentication — 此命令顯示有關AAA TACACS+身份驗證的資訊。 如果使用者輸入的使用者名稱不在TACACS+伺服器上,則身份驗證失敗。以下是debug tacacs authentication命令輸出中的身份驗證失敗:

*Mar 1 00:07:26.624: TPLUS: Queuing AAA Authentication request 0 for processing *Mar 1 00:07:26.624: TPLUS: processing authentication start request id 0 *Mar 1 00:07:26.624: TPLUS: Authentication start packet created for 0(User3) *Mar 1 00:07:26.624: TPLUS: Using server 172.16.1.1 *Mar 1 00:07:26.625: TPLUS(0000000)/0/NB_WAIT/A88784: Started 5 sec timeout *Mar 1 00:07:26.626: TPLUS(0000000)/0/NB_WAIT: socket event 2

```
1 00:07:26.626: TPLUS(0000000)/0/NB_WAIT: wrote entire 25 bytes request
*Mar
*Mar 1 00:07:26.627: TPLUS(0000000)/0/READ: socket event 1
*Mar 1 00:07:26.627: TPLUS(0000000)/0/READ: Would block while reading
*Mar 1 00:07:26.631: TPLUS(0000000)/0/READ: socket event 1
*Mar 1 00:07:26.632: TPLUS(0000000)/0/READ: read entire 12 header bytes (expect 16
bytes data)
*Mar 1 00:07:26.632: TPLUS(0000000)/0/READ: socket event 1
     1 00:07:26.632: TPLUS(0000000)/0/READ: read entire 28 bytes response
*Mar
*Mar 1 00:07:26.632: TPLUS(0000000)/0/A88784: Processing the reply packet
*Mar 1 00:07:26.632: TPLUS: Received authen response status GET_PASSWORD (8)
*Mar 1 00:07:26.632: TPLUS: Queuing AAA Authentication request 0 for processing
*Mar 1 00:07:26.633: TPLUS: processing authentication continue request id 0
*Mar 1 00:07:26.633: TPLUS: Authentication continue packet generated for 0
     1 00:07:26.634: TPLUS(0000000)/0/WRITE/A88784: Started 5 sec timeout
*Mar
     1 00:07:26.634: TPLUS(0000000)/0/WRITE: wrote entire 22 bytes request
*Mar
*Mar 1 00:07:26.688: TPLUS(0000000)/0/READ: socket event 1
*Mar 1 00:07:26.688: TPLUS(00000000)/0/READ: read entire 12 header bytes (expect 6
bytes data)
*Mar 1 00:07:26.689: TPLUS(0000000)/0/READ: socket event 1
*Mar 1 00:07:26.689: TPLUS(0000000)/0/READ: read entire 18 bytes response
     1 00:07:26.689: TPLUS(0000000)/0/A88784: Processing the reply packet
*Mar
     1 00:07:26.689: TPLUS: Received authen response status FAIL (3)
*Mar
```

可以選擇**Reports and Activity > Failed Authentication**以檢視ACS上的身份驗證嘗試失敗。以下是範 例:

<u>Date</u> ♦	<u>Time</u>	Message- <u>Type</u>	<u>User-</u> Name	<u>Group-</u> <u>Name</u>	Caller- ID	<u>Authen-</u> Failure-Code	Author- Failure- Code	Author- Data	NAS- Port
05/17/2006	19:40:14	Authen failed	User3			CS user unknown			

如果您在AP上使用低於Cisco IOS軟體版本12.3(7)JA的Cisco IOS軟體版本,則每次嘗試使用 HTTP登入AP時都可能會碰到錯誤。思科錯誤ID為<u>CSCeb52431(</u>僅限<u>註冊</u>客戶)。

Cisco IOS軟體HTTP/AAA實施要求對每個單獨的HTTP連線進行獨立身份驗證。無線Cisco IOS軟體 GUI涉及在單一網頁內引用多個獨立的檔案(例如Javascript和GIF)。因此,如果您在無線Cisco IOS軟體GUI中載入單一頁面,AAA伺服器可能會收到幾十個不同的驗證/授權要求。

對於HTTP身份驗證,請使用RADIUS或本地身份驗證。RADIUS伺服器仍要承受多個驗證要求。但 RADIUS的可擴充性高於TACACS+,因此可能會提供較小的效能影響。

如果必須使用TACACS+且您有思科ACS,請將**single-connection**關鍵字與**tacacs-server**命令一起使 用。將此關鍵字與命令一起使用會使ACS省去大部分TCP連線建立/拆卸開銷,並可能會在一定程度 上降低伺服器上的負載。

對於AP上的Cisco IOS軟體版本12.3(7)JA及更高版本,軟體包含修復。本節的其餘部分將介紹修復 程式。

使用AAA驗證快取功能可快取TACACS+伺服器傳回的資訊。身份驗證快取和配置檔案功能允許 AP快取使用者的身份驗證/授權響應,以便無需將後續身份驗證/授權請求傳送到AAA伺服器。若要 使用CLI啟用此功能,請使用以下命令: 有關此功能和命令的更多資訊,請參閱<u>管理接入點</u>的<u>配置身份驗證快取和配置檔案</u>部分。

要在GUI上啟用此功能,請選擇**Security > Admin Access**,並選中**Enable Authentication Server Caching**覈取方塊。由於本檔案使用Cisco IOS軟體版本12.3(7)JA,因此本檔案會使用<u>設定</u>所述的修 正程式。

相關資訊

- 設定RADIUS和TACACS+伺服器
- <u>公告:IOS接入點通過請求來轟炸TACACS+伺服器</u>
- 使用RADIUS伺服器的EAP身份驗證
- 無線產品支援
- 技術支援與文件 Cisco Systems