TACACS+ su un access point Aironet per l'autenticazione di accesso con uso della configurazione GUI

Sommario

Introduzione Prerequisiti Requisiti Componenti usati Convenzioni Configurazione Esempio di rete Configurazione del server TACACS+ per l'autenticazione di accesso - Uso di ACS 4.1 Configurazione del server TACACS+ per l'autenticazione di accesso - Uso di ACS 5.2 Configurazione di Aironet AP per l'autenticazione TACACS+ Verifica Verifica per ACS 5.2 Risoluzione dei problemi Informazioni correlate

Introduzione

Questo documento spiega come abilitare i servizi TACACS Plus (TACACS+) su un Cisco Aironet Access Point (AP) per eseguire l'autenticazione di accesso con l'uso di un server TACACS+.

Prerequisiti

Requisiti

Prima di provare questa configurazione, accertarsi di soddisfare i seguenti requisiti:

- Conoscenza di come configurare i parametri di base sugli access point Aironet
- Informazioni su come configurare un server TACACS+ come Cisco Secure Access Control Server (ACS)
- Conoscenza dei concetti di TACACS+

Per informazioni sul funzionamento di TACACS+, fare riferimento alla sezione <u>Descrizione di</u> <u>TACACS+</u> in <u>Configurazione di server RADIUS e TACACS+</u>.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Access point Aironet Cisco Aironet serie 1240/1140
- ACS con software versione 4.1
- ACS con software versione 5.2

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento <u>Cisco sulle convenzioni</u> nei suggerimenti tecnici.

Configurazione

In questa sezione viene spiegato come configurare Aironet AP e il server TACACS+ (ACS) per l'autenticazione dell'accesso basata su TACACS+.

In questo esempio di configurazione vengono utilizzati i seguenti parametri:

- Indirizzo IP dell'ACS-172.16.1.1/255.255.0.0
- Indirizzo IP dell'access point-172.16.1.30/255.255.0.0
- Esempio di chiave segreta condivisa utilizzata sull'access point e sul server TACACS+

Le credenziali dell'utente configurate da questo esempio nel server ACS sono le seguenti:

- Nome utente: User1
- Password—Cisco
- Gruppo—AdminUsers

Ènecessario configurare le funzionalità di TACACS+ per convalidare gli utenti che tentano di connettersi all'access point tramite l'interfaccia Web o l'interfaccia della riga di comando (CLI). Per eseguire questa configurazione, è necessario eseguire i seguenti task:

- 1. <u>Configurare il server TACACS+ per l'autenticazione di accesso</u>.
- 2. Configurare Aironet AP per l'autenticazione TACACS+.

Nota: per ulteriori informazioni sui comandi menzionati in questo documento, usare lo <u>strumento di</u> <u>ricerca</u> dei comandi (solo utenti <u>registrati</u>).

Esempio di rete

Nel documento viene usata questa impostazione di rete:



Configurazione del server TACACS+ per l'autenticazione di accesso - Uso di ACS <u>4.1</u>

Il primo passo è configurare un daemon TACACS+ per convalidare gli utenti che tentano di accedere all'access point. È necessario configurare ACS per l'autenticazione TACACS+ e creare un database utenti. È possibile utilizzare qualsiasi server TACACS+. In questo esempio viene utilizzato ACS come server TACACS+. Attenersi alla seguente procedura:

 Per aggiungere l'access point come client di autenticazione, autorizzazione e accounting (AAA), completare la procedura seguente:Dall'interfaccia utente di ACS, fare clic sulla scheda Network Configuration (Configurazione di rete).In Client AAA, fare clic su Add Entry (Aggiungi voce).Nella finestra Add AAA Client, immettere il nome host dell'access point, l'indirizzo IP dell'access point e una chiave segreta condivisa.La chiave segreta condivisa deve essere uguale alla chiave segreta condivisa configurata nell'access point.Dal menu a discesa Autentica tramite, selezionare TACACS+ (Cisco IOS).Per salvare la configurazione, fare clic su Submit + Restart (Invia + Riavvia).Di seguito è riportato un esempio:

CiscoSecure ACS - N	ficrosoft Internet Explorer	<u>. 6 ×</u>
Ele Edt Yew Fg	varkes Iools Help	Leis » 🏦
Address A http://127.0	3.0.1:1065/	🚽 🔁 🐼
Cisco Statems	Network Configuration	×
latilbuatibu.		🛎 Holp 🖿
Setup	Add AAA Client	AAA Client Hortsone
Broup Setup	AAA Client Hostname AccessPoint	AAA Client IP Address Shared Secret Satured Secret Satured Secret Satured Secret Satured Secret
Retwork Configuration	AAA Client IP Address	Authenticate Using Authenticate Using Single Ceaner/LTACACS+ AAA Cleant Lag Update/Watching Packets from this
Sustem Configuration	Shared Secret Example	AAA Client • Los EADOUS Tometing Packets from this AAA Client • Replace EADOUS Port info with Username
Configuration	RADIUS Key Wrap	From this AAA Cleant • Match Framed IP Address with user IP
Administration Control	Key Encryption Key	address for accounting packets from this AAA Client
External User	Message Authenticator Code Key	
Posture Validation	Key Input Format C ASCII @ Hexadecimal	AAA Client Hostname
Network Access Profiles	Authenticate Using TACACS+ (Cisco IOS)	The AAA Client Hostname is the name assigned to the AAA client.
Reports and	Single Connect TACACS+ AAA Client (Record stop in accounting on failure)	Back to Teel
(Online	Log Update/Watchdog Packets from this AAA Client	AAA Cliest IP Address
Documentation	Log RADIUS Tunneling Packets from this AAA Client	The AAA Client IP Address is the IP address assigned to the
	Replace RADIUS Port info with Username from this AAA Client	AAA client,
	Match Framed-IP-Address with user IP address for accounting packets from this AAA Client	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
	Submit Submit + Apply Cancel	AAA client to be represented by this AAA client entry. To mparts each IP address, press Eater.
1		- Ci

In questo esempio vengono utilizzati: Access point nome host client AAAL'indirizzo 172.16.1.30/16 come indirizzo IP del client AAAEsempio di chiave segreta condivisa

2. Completare questi passaggi per creare un gruppo che contenga tutti gli utenti amministrativi (admin):Fare clic su Group Setup (Imposta gruppo) dal menu a sinistra.Viene visualizzata una nuova finestra.Nella finestra Impostazione gruppo, selezionare un gruppo da configurare dal menu a discesa e fare clic su Rinomina gruppo.In questo esempio viene selezionato il Gruppo 6 dal menu a discesa e viene rinominato il gruppo AdminUsers.Fare clic su Invia.Di seguito è riportato un

esempio:		
CiscoSecure AES - N	ticrosoft Internet Explorer	
Ele Edt Yew Fg	vorites Iools Help	Lets "
Aggress [@] http://127.0	3.0.1:1965y	
Cisco Statems	Group Setup	×
allsalls	Select	Help
User Setup	Renaming Group: Group 6	Rename Group
Network Composeds	Group AdminUsers Submit Cancel	Rename Group Type a new group name and click Subwit to assign a more descriptive name to the group profile. This is useful if different groups have been configured to allow gracific authorization privileges, such
System Configuration	😤 Bask to Hirlp	as PPP or Telest-only capability. Click Cancel to return to the Group Setup window without saving a new group name. [Back to Tap]
Control Cutabases		
Network Access		
Datise Documentation		
1		Internet.

3. Completare questi passaggi per aggiungere gli utenti al database TACACS+:Fare clic sulla scheda Impostazione utente.Per creare un nuovo utente, immettere il nome utente nel campo Utente e fare clic su Aggiungi/Modifica.Di seguito è riportato un esempio che crea User1:



Dopo aver fatto clic su Aggiungi/Modifica, viene visualizzata la finestra Aggiungi/Modifica relativa all'utente.

4. Immettere le credenziali specifiche dell'utente e fare clic su Submit (Invia) per salvare la configurazione.Le credenziali che è possibile immettere includono:Informazioni utente supplementariImpostazione utenteGruppo a cui è assegnato l'utenteDi seguito è riportato un esempio:

CiscoSecure ACS - Mic	rosoft Internet Explorer	X
Ele Edt Yew Favor	ites Iools Help	Links 39 💐
Address () http://127.0.0	.1:10657	a 💽 💌
Cisco Svarens	User Setup	
User Setup Components Components Components Configuration Configuration Configuration Configuration	User: User1 (New User) Account Disabled Supplementary User Info Real Name User1 Description	Account Disabled Ordering a Unername Supplementary User Infe Passmed Authentication Group to which the user is assigned Callback Client IP Address Assignment Advanced Settlings Network Access Restrictions Man Sessions Usage Quetas Access It Lis Advanced TACASS - Settings TACACS - Enable Control
Ecternal User Databases Perfuse Validation	User Setup ? Password Authentication: ACS Internal Database CiscoSecure PAP (Also used for CHAP/MS- CHAP/ARAP, if the Separate field is not	IACAS+ Enable Desenver IACAS+ Enable Desenver TACAS+ Shell Command Authorization Command Authorization for Network Device Management Applications TACAS+ Unknewn Services ILTE RADIUS Attributes BADIUS Yender-Specific Attributes
Commentation	Checked.) Password Confirm Password Separate (CHAP/MS-CHAP/ARAP) Password Confirm Password When a token server is used for authentication, When a token server is used for authentication,	Account Disabled Status Select the Account Disabled check box to disable this account: clear the check box to enable the account. [Back to Top] Deleting a Username The Delete botton appears only when you are editing an existing user account, not when you are adding a new user account. To delete the current user account from the database, click Delete. When asked to
<u>ا</u>	Submit Cancel	[Aark to Ton]

In questo esempio l'utente User1 viene aggiunto al gruppo AdminUsers.



Nota: se non si crea un gruppo specifico, gli utenti vengono assegnati al gruppo predefinito.

5. Per definire il livello di privilegio, completare i seguenti passaggi:Fare clic sulla scheda Impostazione gruppo.Selezionare il gruppo precedentemente assegnato all'utente e fare clic su Modifica impostazioni.In questo esempio viene utilizzato il gruppo AdminUsers.In TACACS+ Settings, selezionare la casella di controllo Shell (exec) e la casella di controllo Privilege level che ha un valore di 15.Fare clic su Invia +



Nota: per essere accessibile come livello 15, il livello di privilegio 15 deve essere definito per la GUI e Telnet. In caso contrario, per impostazione predefinita, l'utente può accedere solo come livello 1. Se il livello di privilegio non è definito e l'utente tenta di accedere alla modalità di abilitazione dalla CLI (con Telnet), l'access point visualizza questo messaggio di errore: AccessPoint>enable % Error in authentication

Ripetere i passaggi da 2 a 4 di questa procedura se si desidera aggiungere altri utenti al database TACACS+. Dopo aver completato questi passaggi, il server TACACS+ è pronto per convalidare gli utenti che tentano di accedere all'access point. A questo punto, è necessario configurare l'access point per l'autenticazione TACACS+.

Configurazione del server TACACS+ per l'autenticazione di accesso - Uso di ACS 5.2

Il primo passaggio è aggiungere l'access point come client AAA nell'ACS e creare una policy TACACS per l'accesso.

1. Per aggiungere un access point come client AAA, completare la procedura

seguente:Dall'interfaccia utente di ACS, fare clic su **Risorse di rete**, quindi su **Dispositivi di rete e client AAA**.In Dispositivi di rete fare clic su **Crea**.Immettere il nome host dell'access point in **Nome** e fornire una descrizione dell'access point.Selezionare la **Posizione** e il **Tipo di dispositivo**, se queste categorie sono definite.Poiché è in corso la configurazione di un solo access point, fare clic su **Indirizzo IP singolo**. È possibile aggiungere l'intervallo di indirizzi IP di più access point facendo clic su **Intervalli IP**. Quindi, immettere l'indirizzo IP dell'access point.In **Authentication Options** (Opzioni di autenticazione), selezionare la casella **TACACS+** e immettere il **segreto condiviso**.Di seguito è riportato un esempio:

* 🚭 My Workspace	Network Resources > 1	NEWOR Devices and AAA Climbs > Oreste							
Ap Reference Personances Network Device Groups Location Device Type	Name A Description A Network Device 0	P1140 utonomous AP 1140 ut Soor 1 Srouges							
Default Network Device External REOL IS Servers	Locidon	All Locations	Belect						
 B Users and identity Stores 	Device Type	All Device Types	Select						
+ Q. Policy Elements	IP Address			Authentication Options					
+ 🔓 Access Policies	🖷 🖉 Single IP	Address 🕐 IP Range(s)		- TACACE- 2					
• 🔄 Monitoring and Reports	• P. 172161	00		Shared Secret cisco					
System Administration			Legacy TRCACS+ Single Connect Support TRCACS+ Draft Compliant Single Connect Support RADUS						
	o = Required felt	8 - 19 - 19 - 19 - 19 - 19 - 19 - 19 - 1							

2. Il passaggio successivo consiste nella creazione di un nome utente e di una password di accesso:Fare clic su Utenti e archivi identità, quindi su Utenti.Fare clic su Crea.Specificare il nome utente in Nome e fornire una descrizione.Selezionare l'eventuale gruppo di identità.Immettere la password sotto la casella di testo Password e immetterla nuovamente sotto Conferma password.Èpossibile modificare la password di abilitazione immettendo una password in Abilita password. Immettere nuovamente per confermare.Di seguito è riportato un

esempio:

 Ty My Workspace 	sers and klentify Stores + Internal klentify Stores + Usin s + Create				
Si Alebook Resources Identify Orsups Identify Orsups Honols Honols	Conservat Name: cscol23 Babas: [nabled •] Description: Legin for Autonomoust AP I dentity Oroups AI Oroups Beter	Esable Password Into Password must • Contain 4 - 32 Enable Password Confirm Password	ematum characters		
C Moniforing and Reports Bystem Administration	rere are no additional identity attrautes defined for user records			No. of Concession, Name	

3. Per definire il livello di privilegio, completare i seguenti passaggi:Fare clic su **Elementi criteri** > **Autorizzazioni e autorizzazioni > Amministrazione dispositivi > Profili shell**.Selezionare la

casella di controllo **Permetti accesso** e fare clic su **Duplica**.

CISCO CISCO OCCURO		
No Network Resources		
Series and identify Stores	Shell Profiles	Showing f-f of f 50 + per page Go
· O. Poley Liments	Filer whath E w 00 w	
Session Conditions Date and Time Custom Nétwork Conditions	Rame - Description Permi Access	
Adherication and Permissions Network Access Dence Administration Command Sets Named Permission Objects		
> 🔓 Access Policies		
Monitoring and Reports		
 System Administration 		
	Create Duptrate Edt. Delete	(H) (H) Page 1 of (H) (H)

Inserire il **nome** e la **descrizione**.

cisco Cisco Secure A	cs	at a sector of	expressional2 (Primary)	Log Dat About Help
• 💮 MyWorkspace	Policy Elements + Authorization and Pentilisions + Device Administration + Shell Publish + Duplicate: "Penet Access"	a se	Marine State	
Section Conditions	General Common Tasks Custom Atributes Name: Autonomous AP Description: TACACS+ login for Autonomous AP			
Date and Time Custom - Network Conditions - Authorization and Permissions - Network Access - Device Administration - Command Sets - Stored Database	Prequed faits			
+ 🕞 Access Policies				
• 📳 Monitoring and Reports				
 Weishern Administration 				

Selezionare la scheda Task comuni e scegliere **15** per il privilegio Massimo.

 MyWorkspace 	Policy Denents > Authorization a	and Permissions	+ Device	Administra	tion × Shell Profiles	+ Delicite Th	eest Access*			
Construction of the sector of the secto	Omerai Common las Phologe Lawi Default Privilege IV Maximum Privilege IV Shill Attributes Access Control List II Auto Command IV No Escape IV No Hang Up IV Timeout IV Caliback Line IV Caliback Line IV Caliback Line IV Caliback Line IV	Notin Use - State - Notin Use -	Value	15 v 15 v 15 z 1 z 2 z 3 4 5 5 7 8 9 10 11 12 13 14 15 16 17 17 18 16 17 17 18 19 19 19 19 19 19 19 19 19 19						

Fare clic su Invia.

4. Per creare un criterio di autorizzazione, completare i seguenti passaggi:Fare clic su Access Policies > Access Services > Default Device Admin > Authorization.Per creare un nuovo criterio di autorizzazione, fare clic su Crea.Viene visualizzato un nuovo popup per creare le regole per il criterio di autorizzazione.Selezionare il gruppo di identità, la posizione e così via per il nome utente e l'eventuale client AAA.Fare clic su Seleziona per il profilo di guscio per scegliere il profilo creato dall'access point

autonomo.

ababi com como tec	Cisco Secure ACS - Moolla Freeba	a vajmaniace\$2 (Primary) Log Dat About	Hep
cisco Cisco Secure ACS	Emperil 19.106.127.39 Decedmin PolicyInpublicities. do		
Access Failor My Workspace More and Identify Stores More and Identify Stores Policy Elements Access Failor More and Identify Stores More and Identify More and Ide	General Name: Autonomous AP Status: Enabled Image: Autonomous AP Status: Enabled Image: Discontinue button in the lower right area of the policy rules screen controls which policy conditions and results are available here for use in policy rules. Conditions Identify Orsup: -ANA NO0_Location: -ANA NO0_Location: -ANA The Autonomous AP Bellect.		
- Creation Save Char		Customice Hill Court	

Al termine, fare clic su **Salva modifiche**.Fare clic su **Default Device Admin**, quindi su **Protocolli consentiti**.Selezionare **Allow PAP/ASCII**, quindi fare clic su **Submit** (Invia).Fare clic su **Service Selection Rules** (Regole di selezione servizio) per verificare che esista una regola corrispondente a TACACS che punta ad Default Device Admin (Amministratore dispositivo predefinito).



Configurazione di Aironet AP per l'autenticazione TACACS+

Per abilitare le funzionalità TACACS+ sull'access point Aironet, è possibile usare la CLI o la GUI. Questa sezione spiega come configurare l'access point per l'autenticazione TACACS+ con l'uso della GUI.

Completare questa procedura per configurare TACACS+ sull'access point con la GUI:

 Completare questa procedura per definire i parametri del server TACACS+:Dalla GUI dell'access point, scegliere Sicurezza > Server Manager.La sicurezza: Viene visualizzata la finestra Server Manager.Nell'area Server aziendali selezionare TACACS+ dal menu a discesa Elenco server correnti.Nella stessa area, immettere l'indirizzo IP, il segreto condiviso e il numero della porta di autenticazione del server TACACS+.Fare clic su Apply (Applica).Di seguito è riportato un esempio:

Cisco 105 Series AP - Security	y - Server Manager - Microsoft	Internet Exp	lorer provided by Cisco Sy:	stems, Inc.	
Ble Edit Yew Pavorites	Icols Help				- 10 C
🕹 Back + 🔿 + 🕥 😭 🚮	Gifearch 🕞 Favorites 🤿	teda 🥑	👌 🖉 🖾 🕑 🎱 📖		
Address () http://10.77.244.194	ap_sec_network-security_a.shtml#	CorpServers			● (PGo Unks ¹⁰
Cited Streems	100000				
	Cisco	Airon	et 1240AG Seri	es Access Point	ba ≝
	SERVER MANAGER		GLOBAL PROPERTIES		
HOME	,				
EXPRESS SET-UP	Hostname ap				ap uptime is 2 hours, 53 minutes
NETWORK MAP. +					
ASSOCIATION +	Security: Server Manager				
NETWORK +	Backup RADIUS Server				
SECURITY	and a second second	_		_	
Admin Access	Backup RADIUS Server:			(Hostname or IP Address)	
Encryption Manager	Shared Secret:				
SSID Manager	Sharew Secret				
Server Manager					Apply Delete Cancel
AP Addientication	Comorate Servers				
Local RADIUS Server	corporate service				
Advanced Security	Current Server List				
SERMCES +	TACACS.				
WIRELESS SERVICES +		Server		1721611	(Hostname or IP Address)
EVENTLOG +	4 NEW 5				(noninane or a resource)
		Shared	Secret:		
	Delete	Authen	tication Port (optional):	49 (0-65536)	
		Account	ting Part (antional):	DISABLED O COST	
		ACCOUNT	ang rorr (opuonal):	(0-65536)	
					Apply Cancel
(a)					internet

Nota: per impostazione predefinita, TACACS+ usa la porta TCP 49.**Nota:** la chiave segreta condivisa configurata sull'ACS e sull'access point deve corrispondere.

 Scegliere Priorità predefinite server > Autenticazione amministratore (TACACS+), selezionare dal menu a discesa Priorità 1 l'indirizzo IP del server TACACS+ configurato e fare clic su Applica.Di seguito è riportato un esempio:

Cisco 105 Series AP - Security	y - Server Manager - Microsoft I	Internet Explorer provided by Cisco Sy	stems, Inc.		X
Ele Edit Yew Pavorites	Toola Rep				100
4=Back • ⇒ - 🥥 🔂 🖽	Search @Favorites 😚	keda 🎯 🔂 - 🎝 📼 🖃 🍪 📖			
Address http://10.77.244.194	ap_sec_network-security_a.shtml#	CorpServers		- e	Go Links ³⁰
					<u> </u>
	Delete	Authentication Port (optional):	49 (0-65536)		
		Accounting Port (optional):	DISABLED (0-65536)		1
				Apply Can	cel I
				. 499	
	Default Server Priorities				
	EAP Authentication	MAC Authentic	ation	Accounting	
	Priority 1: NONE > .	Priority 1: KNC	DNE > 💌	Priority 1: < NONE > .	
	Priority 2: (NONE)	Priority 2: < NC	DNE > 💌	Priority 2: (NONE)	
	Priority 3: (NONE)	Priority 3: KNC	ONE > •	Priority 3: (NONE)	
		, .	_		
	Admin Authentication (R/	ADIUS) Admin Authent	ication (TACACS+)		
	Priority 1: (NONE)	Priority 1: 172	16.1.1		
	Divity 2 (NONE)	Drivity 2 KN	INE > .		
	Printy 2 Print 2	Phony 2. [The			
	Priority 3: CNUNE >	Priority 3: [4 N.	NE 1		
				Apply Can	cel
					_
Close W	ndow			Copyright (c) 1992-2006 by Cisco Syst	ems, Inc.
10)					
				ancernet	

 Scegliere Protezione > Accesso amministratore e, per Autenticazione amministratore tramite:, scegliere Solo server di autenticazione e fare clic su Applica.Questa opzione garantisce che gli utenti che tentano di accedere all'access point vengano autenticati da un server di autenticazione.Di seguito è riportato un esempio:



Questa è la configurazione CLI dell'esempio di configurazione:

```
AccessPoint
AccessPoint#show running-config
Current configuration : 2535 bytes
1
version 12.3
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
1
hostname AccessPoint
!
1
ip subnet-zero
!
1
aaa new-model
!--- Enable AAA. ! ! aaa group server radius rad_eap !
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
server tacacs+ tac_admin
!--- 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 bridge-
group 1 bridge-group 1 subscriber-loop-control bridge-
group 1 block-unknown-source no bridge-group 1 source-
learning 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-loop-
control bridge-group 1 block-unknown-source no bridge-
group 1 source-learning no bridge-group 1 unicast-
flooding 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 source-
learning bridge-group 1 spanning-disabled ! interface
BVI1 ip address 172.16.1.30 255.255.0.0 no ip route-
cache ! 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 tacacs-
server 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
```

Nota: per il corretto funzionamento di tutti i comandi in questa configurazione, è necessario disporre del software Cisco IOS versione 12.3(7)JA o successive. In una versione precedente del software Cisco IOS, tutti questi comandi potrebbero non essere disponibili.

Verifica

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

Lo <u>strumento Output Interpreter</u> (solo utenti <u>registrati</u>) (OIT) supporta alcuni comandi **show**. Usare l'OIT per visualizzare un'analisi dell'output del comando **show**.

Per verificare la configurazione, provare ad accedere all'access point con la GUI o la CLI. Quando si tenta di accedere al punto di accesso, il punto di accesso richiede un nome utente e una password.

Enter Nets	work Passwor	d ?×
? >	Please type yo	our user name and password.
8	Site:	172.16.1.30
	Realm	level_1_access
	User Name	User1
	Password	****
	🔲 Save this p	password in your password list
		OK Cancel

Quando si forniscono le credenziali dell'utente, l'access point inoltra le credenziali al server TACACS+. Il server TACACS+ convalida le credenziali sulla base delle informazioni disponibili nel proprio database e fornisce l'accesso all'access point in caso di autenticazione riuscita. È possibile scegliere **Report e attività > Autenticazione passata** su ACS e utilizzare il report Autenticazione passata per verificare se l'autenticazione per l'utente è riuscita. Di seguito è riportato un esempio:



Èpossibile anche usare il comando **show tacacs** per verificare la corretta configurazione del server TACACS+. Di seguito è riportato un esempio:

AccessPoint#**show tacacs**

Tacacs+	Server	:	172.16.1.1/49
	Socket open	ns:	348
	Socket close	es:	348
	Socket abort	ts:	0
	Socket error	rs:	0
	Socket Timeout	ts:	0
Faile	ed Connect Attempt	ts:	0
	Total Packets Ser	nt:	525

Verifica per ACS 5.2

Èpossibile verificare i tentativi di accesso non riusciti/superati per le credenziali da ACS 5.2:

- 1. Fare clic su **Monitoraggio e report > Avvia Visualizzatore report e monitoraggio**.Viene visualizzato un nuovo popup con il quadro comandi.
- 2. Fare clic su **Authentication-TACACS-Today**. Mostra i dettagli dei tentativi non riusciti/superati.

Risoluzione dei problemi

Èpossibile usare questi comandi di debug sull'access point per risolvere i problemi relativi alla configurazione:

Nota: consultare le <u>informazioni importanti sui comandi di debug</u> prima di usare i comandi di **debug**.

• debug tacacs events: questo comando visualizza la sequenza di eventi verificatisi durante l'autenticazione TACACS. Di seguito è riportato un esempio dell'output di questo comando: *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
*Mar 1 00:51:21.116: TPLUS(0000000)/0/NB_WAIT: socket event 2
*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
     1 00:51:21.117: TPLUS(0000000)/0/READ: Would block while reading
*Mar
*Mar 1 00:51:21.120: TPLUS(0000000)/0/READ: socket event 1
*Mar 1 00:51:21.120: TPLUS(00000000)/0/READ: read entire 12 header bytes (expect
16 bytes data)
*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 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
*Mar 1 00:51:21.122: TPLUS(0000000)/0/WRITE: wrote entire 22 bytes request
*Mar 1 00:51:21.178: TPLUS(0000000)/0/READ: socket event 1
     1 00:51:21.178: TPLUS(0000000)/0/READ: read entire 12 header bytes (expect
*Mar
6 bytes data)
*Mar 1 00:51:21.178: TPLUS(0000000)/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: utilizzare questo comando per risolvere i problemi di autenticazione HTTP. Il comando visualizza il metodo di autenticazione tentato dal router e i messaggi di stato specifici dell'autenticazione.
- debug aaa authentication: questo comando visualizza informazioni sull'autenticazione AAA TACACS+.

Se l'utente immette un nome utente che non esiste sul server TACACS+, l'autenticazione non riesce. Di seguito è riportato l'output del comando **debug tacacs authentication** per un'autenticazione non riuscita:

```
*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
*Mar 1 00:07:26.626: TPLUS(0000000)/0/NB_WAIT: wrote entire 25 bytes request
*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
*Mar 1 00:07:26.632: TPLUS(00000000)/0/READ: read entire 28 bytes response
     1 00:07:26.632: TPLUS(0000000)/0/A88784: Processing the reply packet
*Mar
*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
*Mar 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
     1 00:07:26.688: TPLUS(0000000)/0/READ: socket event 1
*Mar
*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
*Mar 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)
```

Per visualizzare il tentativo di autenticazione non riuscito su ACS, scegliere **Report e attività > Autenticazione non riuscita**. Di seguito è riportato un esempio:

<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			

Se si usa una versione software Cisco IOS sull'access point precedente al software Cisco IOS versione 12.3(7)JA, è possibile che venga riscontrato un bug ogni volta che si cerca di accedere all'access point con il protocollo HTTP. L'ID bug Cisco è <u>CSCeb52431</u> (solo utenti <u>registrati</u>).

L'implementazione HTTP/AAA del software Cisco IOS richiede l'autenticazione indipendente di ciascuna connessione HTTP separata. L'interfaccia grafica wireless del software Cisco IOS include il riferimento di molte dozzine di file separati all'interno di una singola pagina Web (ad esempio Javascript e GIF). Pertanto, se si carica una singola pagina nell'interfaccia grafica wireless del software Cisco IOS, dozzine e dozzine di richieste separate di autenticazione/autorizzazione possono raggiungere il server AAA.

Per l'autenticazione HTTP, utilizzare RADIUS o l'autenticazione locale. Il server RADIUS è ancora soggetto alle richieste di autenticazione multiple. RADIUS è tuttavia più scalabile di TACACS+ ed è quindi probabile che produca un impatto meno negativo sulle prestazioni.

Se si deve usare TACACS+ e si ha un Cisco ACS, usare la parola chiave **single-connection** con il comando **tacacs-server**. L'uso di questa parola chiave con il comando elimina la maggior parte del sovraccarico di configurazione/disinstallazione della connessione TCP e probabilmente riduce il carico sul server in una certa misura.

Per il software Cisco IOS versione 12.3(7) JA e successive sull'access point, il software include una correzione. Nella parte restante di questa sezione viene descritta la correzione.

Usare la funzione di cache di autenticazione AAA per memorizzare nella cache le informazioni restituite dal server TACACS+. La funzione di profilo e cache di autenticazione consente all'access point di memorizzare nella cache le risposte di autenticazione/autorizzazione per un utente in modo che le successive richieste di autenticazione/autorizzazione non debbano essere inviate al server AAA. Per abilitare questa funzione dalla CLI, usare questi comandi:

cache expiry cache authorization profile cache authentication profile aaa cache profile

Per ulteriori informazioni su questa funzione e sui comandi, consultare la sezione <u>Configurazione</u> <u>della cache e del profilo di autenticazione</u> in <u>Amministrazione dell'access point</u>.

Per abilitare questa funzione sulla GUI, selezionare **Security > Admin Access** (Sicurezza > Accesso amministratore) e selezionare la casella di controllo **Enable Authentication Server Caching** (Abilita cache server di autenticazione). Poiché questo documento utilizza il software Cisco IOS versione 12.3(7)JA, viene usata la correzione, come mostrato nelle <u>configurazioni</u>.

Informazioni correlate

- <u>Configurazione dei server RADIUS e TACACS+</u>
- Field Notice: IOS Access Point Bombard il server TACACS+ con richieste
- <u>Autenticazione EAP con server RADIUS</u>
- Supporto dei prodotti wireless
- Documentazione e supporto tecnico Cisco Systems