# 使用ACS服务器在Cisco ONS15454/NCS2000上 配置TACACS+

### 目录

<u>简介</u> <u>先决条件</u> <u>要求</u> 使用的组件 配置 验证 故障排除

# 简介

本文档介绍如何在ONS15454/NCS2000设备和思科访问控制系统(ACS)上配置终端访问控制器访问 控制系统(TACACS+)的分步说明。 所有主题都包括示例。本文档中提供的属性列表并非详尽或权威 ,在不更新本文档的情况下随时可能更改。

### 先决条件

#### 要求

Cisco 建议您了解以下主题:

- •思科传输控制器(CTC)GU
- ACS服务器

#### 使用的组件

本文档不限于特定的软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原 始(默认)配置。

**注意:**如果您的网络处于活动状态,请确保您了解所有命令的潜在影响。

#### 配置

ONS15454/NCS2000所需的配置:

1.您可以从此选项卡配置TACACS服务器配置。导航**至Provisioning > Security > TACACS** Server,如图所示。

Tab View	/ _×
Alarms Conditions History Circuits Provisioning Inventory Maintenance	
General Users Active Logins Policy Data Comm Access RADIUS Server FACACISS Cover Legal Disclaimer	
Network	
OS Enable TACACS Authentication	Apply
Protection I Enable node as Final Authenticator when no TACACS+ Server is reachable	Reset
SECURITY TACACS Servers in Order of Authentication	Help
Commo Channells Node Address Shared Secret Authentication P	
Alarm Profiles	
Defaults	
WDM-ANS	
SAAN	
CFM Profiles	
Create Edit Delete Move Up Move Down	
	J

#### 2.要添加TACACS+服务器详细信息,请单击"创建"**按**钮。它将打开TACACS+配置窗口,如下图所 示。

Edit TACACS+ Server Entry	×
Node Address:	10.64.106.24
Shared Secret:	CISCO123
Authentication Port:	49
OK	Cancel

- 输入服务器IP地址
- 在节点和TACACS+服务器之间添加共享密钥
- •添加身份验证端口号。在此端口上,TACACS+服务器正在侦听客户端。默认端口号为49

Alarms Conditions	History Circuits Provisioning Inventory Maintenance	
General		
Network	Users Active Logins Policy Data Comm Access RADIUS Server TACAUS Server Legal Dischamer	
RO		Annhy
Protection	Enable TACACS Authentication	white
Consults	C Enable node as Final Authenticator when no TACACS+ Server is reachable	Reset
Steamy	TACACS Servers in Order of Authentication	Help
SOUTHP	Node Address Shared Secret Authentication P	
Comm Channels	16.64.106.74 (190.0123 49	
Alarm Profiles		
Defaults		
WDM-ANS		
SVLAN		
CFM Profiles		
	Create Edit Delete Move Up Move Down	
I I		

3.要激活NODE上的TACACS+服务器配置,请选中**启用TACACS身份验证**复选框,然后单击**应用**按 钮,如图所示。

Enable TACACS Authentication

4.要启用节点作为最终身份验证器,当无法访问任何服务器时,请点击图像所示的复选框。

Enable node as Final Authenticator when no TACACS+ Server is reachable.

5.要修改特定服务器配置,请选择相应的服务器配置行,单击"编辑"按钮以修**改配**置。

6.要删除特定服务器配置,请选择相应的服务器配置行,单击"删**除"**按钮以删除配置。

ACS服务器上所需的配置:

1. 创建网络设备和AAA客户端,然后单击Network Resources(网络资源)**窗格中的Create**按钮 ,如图所示。



2. 提供与ONS**节点配**置中给定的相同的共享密钥。否则,身份验证将失败。

All Locations Select evice Type All Device Types Select Address OIP Subnets OIP Range(s) ■ Single IP Address OIP Subnets OIP Range(s) ■ IP: 10.64.106.156 ■ IP: 10.64.106.156 ■ Connect Device ● Legacy TACACS+ Single Connect Suppor TACACS+ Draft Compliant Single Connect ■ RADIUS OILS Shared Secret: Shore Shared Secret: Shore ■ Legacy TACACS+ Single Connect Suppor ■ TACACS+ Draft Compliant Single Connect ■ Legacy TACACS+ Single Connect Suppor ■ TACACS+ Draft Compliant Single Connect ■ Legacy TACACS+ Single Connect Suppor ■ TACACS+ Draft Compliant Single Connect ■ Legacy TACACS+ Single Connect Suppor ■ TACACS+ Draft Compliant Single Connect ■ Legacy TACACS+ Single Connect Suppor ■ TACACS+ Draft Compliant Single Connect ■ Legacy TACACS+ Single Connect Suppor ■ TACACS+ Draft Compliant Single Connect ■ Legacy TACACS+ Single Connect Suppor ■ TACACS+ Draft Compliant Single Connect ■ Legacy TACACS+ Single Connect Suppor ■ TACACS+ Draft Compliant Single Connect ■ Legacy TACACS+ Single Connect Suppor ■ TACACS+ Draft Compliant Single Connect ■ Legacy TACACS+ Single Connect Suppor ■ TACACS+ Draft Compliant Single Connect ■ Legacy TACACS+ Single Connect Suppor ■ TACACS+ Draft Compliant Single Connect Support ■ TACACS	All Location All Locations evice Type All Device Typ Address	s	Select	
Device Type All Device Types     P Address   Single IP Address IP Subnets IP Subnets IP Range(s) IP: 10.64.106.156 Authentication Options TACACS+ ☑ Shared Secret: CISCO123 Hide Single Connect Device © Legacy TACACS+ Single Connect Suppor TACACS+ Draft Compliant Single Connect Support TACACS+ D	Device Type All Device Typ P Address	\$	Select	
P Address       IP Subnets       IP Range(s)       Authentication Options         ● IP: 10.64.106.156       ● IP Subnets       IP Range(s)       ● TACACS+       ●         ● IP: 10.64.106.156       ● Legacy TACACS+ Single Connect Device       ● Legacy TACACS+ Single Connect Support       ● TACACS+ Draft Compliant Single Connect         ● RADIUS       ●       ● Shared Secret:       ● Shared Secret:       ● Shared Secret:       ● Shared Secret:       ● RADIUS         ● RADIUS       ●       ● Shared Secret:       ● RADIUS       ●         ● Key Unput Format       ● ASCIIII ● HEXADECIMINATION FORMATION FOR	P Address			
Single IP Address IP Subnets IP Range(s) TACACS+ IP Shared Secret: CISCO123 Hide Single Connect Device Legacy TACACS+ Single Connect Support TACACS+ Draft Compliant Single Connect RADIUS Shared Secret: Sho CoA port: 1700 Enable KeyWrap Key Encryption Key: Message Authenticator Code Key: Key Input Format ASCII HEXADECIM				Authentication Options
IP: 10.64.106.156     Shared Secret: CISCO123 Hide     Single Connect Device     UEgacy TACACS+ Single Connect Suppor     TACACS+ Draft Compliant Single Connect     RADIUS     RADIUS     Shared Secret:	Single IP Address O IP S	bnets 💿 IP Range(s)		▼TACACS+
Single Connect Device  Current Connect Device  Current Compliant Single Connect Suppor  TACACS+ Draft Compliant Single Connect  RADIUS  RADIUS  Shared Secret: Sho CoA port: 1700  Enable KeyWrap Key Encryption Key: Key Input Format ASCII © HEXADECIM	6 IP: 10.64106156			Shared Secret: CISCO123 Hide
				Single Connect Device
TACACS+ Draft Compliant Single Connect RADIUS Shared Secret: CoA port: 1700 Enable KeyWrap Key Encryption Key: Message Authenticator Code Key: Key Input Format ASCII  HEXADECIM				Legacy TACACS+ Single Connect Support
RADIUS     Shared Secret:				TACACS+ Draft Compliant Single Connect Support
Shared Secret Sho CoA port: 1700 Enable KeyWrap Key Encryption Key. Message Authenticator Code Key. Key Input Format ASCII HEXADECIM				- RADIUS
CoA port: 1700 Enable KeyWrap Key Encryption Key: Message Authenticator Code Key: Key Input Format ASCII I HEXADECIM				Shared Secret: Show
Enable KeyWrap Key Encryption Key. Message Authenticator Code Key. Key Input Format ASCII I HEXADECIM				CoA port: 1700
Key Encryption Key. Message Authenticator Code Key. Key Input Format O ASCII O HEXADECIM				Enable KeyWrap
Message Authenticator Code Key: Key Input Format 💿 ASCII 🐵 HEXADECIM				Key Encryption Key:
Key Input Format 💿 ASCII 💿 HEXADECIM				Message Authenticator Code Key:
				Key Input Format 💿 ASCII 💿 HEXADECIMAL
Required fields	Required fields			

3.如图所示,在"用户和身份库"Pan中为需要通过身份验证**的用户创建**用户名和密码。



Users and identity Stores	> Internal Identity Stor	es > Users > Create				
General						
O Name:	raamu	Status: Enable	d 🕶 😝			
Description:						
Identity Group:	All Groups		Select			
Email Address:						
Account Disable						
Disable Accou	int if Date Exceeds:	2015-Nov-21 🔟 (уууу-Мт	m-dd)			
🗐 Disable accou	int after 3 succe	ssive failed attempts				
December Hack						
Password Hash	vassword nasn Annlinshle only for Internal I I sars to store nassword as hash					
🖾 Enable Passw	vord Hash	Authentication types	CHAP/MSCHAP will not work if this	option is enabled.		
		while disability the	nash, ensure inacpassword is reco	mgureu using change passworu opion.		
Password Lifetime	•	C	and blacking in some state and			
Password Nev	ver Expired/Disabled	Overwrite's User ac	count blocking in case password ex	prreducisacied		
Password Inform	ation			Enable Password Information		
Password must				Password must		
Contain 4	- 32 characters			<ul> <li>Contain 4 - 128 characters</li> </ul>		
Password Type	E.	Internal Users	Select	Enable Password:		
Password:		•••••		Confirm		
Confirm Passw	vord:			r approva.		
🔲 Change pa	ssword on next login					
User Information						
Thorn one no od	diseast identity while		da.			
Submit Cancel						

4. 在"策略元素"(Policy Elements)窗格中创建外壳配置文件:

a.选择权限级别(0到3):

- 0,用于检索用户。
- 1用于维护用户。
- 2用于调配用户。
- 3(超级用户)。
- b.在"客户属性"面板中**为"空闲**时间"属**性创建自**定义属性。



eneral Common	Tasks Custom	Attributes		
rivilege Level				
Default Privilege:	Static 🗸	Value 2	•	
Maximum Privilege:	Not in Use 👻			
hell Attributes				
Access Control List:	Not in Use 🔻			
Auto Command:	Not in Use 👻			
No Callback Verify:	Not in Use 👻			
No Escape:	Not in Use 👻			
No Hang Up:	Not in Use 👻			
Timeout:	Not in Use 👻			
ldle Time:	Not in Use 👻			
Callback Line:	Not in Use 👻			
Callback Rotary:	Not in Use 👻			
= Required fields				

空闲**时间"**0"表示连接永不超时,并且将永远超时。如果用户指定任何其他时间,则连接将可用这**么** 多秒。

eneral C	ommon Tasks	Custom Attributes		
ommon Tas	ks Attributes			
Attribute		Requirement	Value	
Assigned Pr	vilege Level	Mandatory	2	
anually Ente	ered			
Attribute		Requirement	Value	
dletime		Mandatory	0	
Add A	Edit V	Replace A Delete	Bulk Edit	
ttribute:		_		
equirement	Mandatory 🛨			
ttribute	Static 🚽			
alue:				
omit 📔 Ca	ncel			

5. 在"访问策略"面板中创建访问策略:



a.单击"服**务选择规则**"并创建规则:

- 选择TACACS作为协议
- 设备为All设备或与之前创建的设备类似的特定设备
- 服务类型为Default Device Admin。

Cisco Secure ACS - Mozilla Fi	refox					×
Attps://10.201.229.210/a	csadmin/PolicyInp	utAction.do	0			
General Name: Rule-4	Status:	Enabled	• 0			
The Custo policy cond	mize button in ti ditions and resu	he lower ri Ilts are ava	ight area of the polic ailable here for use i	y rules screen o in policy rules.	controls which	
Conditions	us at a la		T		alaat	
Protocol:	match	•	Tacacs	S	elect	
Results Service: Default Device	e Admin					

b.选择Authorization并在Default Device Admin单选按钮下创建用于授权的规则:

- •选择"已**创建的壳**配置文件"
- •选择特定设备或设备类型中的所有设备



Cisco Secure ACS - Mozilla Firefox	ĸ	
Attps://10.201.229.210/acsad	Imin/PolicyInputAction.do	
General		
Name: Rule-3	Status: Enabled 👻 🕙	
The Customize policy condition	e button in the lower right area of the policy rules screen controls which ins and results are available here for use in policy rules.	
Conditions		
🔲 Identity Group: -AN	Y-	
NDG:Location: -AN	Y-	
NDG:Device Type: in	All Device Types     Select	
Time And Date: -AN	Y-	
Results		
Shell Profile: TACACS-NOD	DE-156 Select	
OK Cancel	)	Help

## 验证

当前没有可用于此配置的验证过程。

# 故障排除

目前没有针对此配置的故障排除信息。