Tacacs **韦家宁** 2020-05-20 发表

# 组网及说明

本案例使用S1850交换机部署hwtacacs,与IMC TAM进行联动,达到安全管理设备的效果。 IMC版本为PLAT 7.3 E0506P03

S1850版本信息如下: H3C Comware Platform Software Comware Software, Version 5.20.99, Release 1102 Copyright (c) 2004-2017 New H3C Technologies Co., Ltd. All rights reserved. H3C S1850-28P uptime is 0 week, 5 days, 6 hours, 8 minutes

H3C S1850-28P 128M bytes DRAM 32M bytes Flash Memory Config Register points to Flash

Hardware Version is Ver.A Bootrom Version is 102 [SubSlot 0] 24GE+4SFP Hardware Version is Ver.A

#### 配置步骤

IMC TAM部署有如下要点: 1、授权场景条件: 设备区域管理、设备类型管理、授权时段策略管理 2、授权命令配置: Shell profile配置、命令集配置 3、设备管理: 配置共享密钥、绑定设备区域、绑定设备类型 4、添加用户名、密码

交换机部署hwtacacs

配置关键点

ISC Management Center		相称 我願	HP-	165	88	SIN.	MAGINIT		
Level and Level	>	門用户>设备用户集整管理>	も 増加用户 前 所有用户			1000			
後用戶管理	>	设备类型信息		UB LOY					
發用戶算點管理	~	类型名称 *	1. 日入用中						
履 快速入门		父亲自然的	设备用户管理	- 101					
<b>13、</b> 授权策的管理			04670-1002	19 <b>1</b> 1	•				
		描述	宋武陵入靈證		•	B 190.948	管理		
授权场最条件						10000-087	-	- 1	
授权命令配置						3 i2011			ika: Koni
· · · · · · · · · · · · · · · · · · ·						LDAP业物管	92		
9						业务争数起意	8		

#### 添加"设备区域管理"



HBC Management Center		ma	900	RP.	985	659	<b>E</b> A	3556107 <b>2</b>	
用戶管理	2	ପ୍ର /Be > ହେଲ/ସ		2005日日本	= > 10.041EM01	ttll > Matolik	新区域		
设备用户管理	$\rightarrow$	设备区域信息							
设备用户并能管理	~	区域名称•			内原	核心设备		1	
<ul> <li>- 夏 快速入门</li> <li>- 9, 授权策略管理</li> <li>- 按权场最余件</li> </ul>		父区域名称 振送					-		
<ul> <li>12(50) (14) (14) (14) (14) (14) (14) (14) (14</li></ul>									462 835
來成該入管理	2								

## 设置"设备类型管理"

Management Center				100	200			ATO A TALE		
8戶管理	>	2用户 > 设备用	户承给管理;	10 単加用户 公 所有用户						
2条用小管理	>	授权场景条件		● 用中朝た田市						
2個用户等的管理	×			と 明入用中 た 新日本の新聞			Baj			(I)
展 快速入门			71	设备用户管理						51
马 经纪律赔偿理			设备区域管	设备用户策略管理 未实施入管理		•		51		授印时经纬期管理
授权场關係得							1800/688-011		•	CI SHOKHING
• 授权命令配置							(現代から配置 売、設備性効		,	PI COMPERSION
- 5 设备管理							LDAP1と特徴を		:	F. Construction
LDAP业务管理										
业务参数配置										
构成这人管理	>									

## 增加

HBC Intelligent ManagementCenter		前向	9000	Ш°	11655	65	16A	系统管理
用戶管理	>	1月中 > 设备用	户策略管理:	授权场最条件	> 设备类型制	59 <u>0</u>		
设备用户管理	>	nta Rivi						
设备用户策略管理	~	10 全部展开10 1	全部收缩					
一 厦 快速入门		类型名称			50	迷		
马 授权策略管理		H3C-V7			н	3C V7版本		
• 授权场置条件								
• 授权命令配置								
- 5 设备管理								
▶ LDAP业务管理								
• 业务参救配置								
来宾接入管理	>							

#### 设置"授权时段策略管理"

HBC Intelligent Center		2551 <b>7020</b>	180° x16%	68	184 - 1869B	
用户管理	>	1日 用か > 设备用の原題管理 >	10 第111月0 日 日 日 日 日 日 日 日 日 日 日 日 日 日 日 日 日 日 日			
设备用户管理	>	atte servi	王 用户就能回意			
设备用户领路管理	×	B 全形現开 B 全形収缩	▲ 导入用户 和 粉色粉的繁荣			
- 厦 快速入门		类型名称	设备用户管理			
· 9, 授权策略管理		H3C-V7	设备用户第吨管理 来器格入管理		開 快速入门	
<ul> <li>11日初の今春2回</li> <li>日、日、日、日、日、日、日、日、日、日、日、日、日、日、日、日、日、日、日、</li></ul>					協会命令監護 う。投発管理 LDAP社会管理 业分学校定置	
20080-0612						

增加,设置"授权时段策略名称"、"生效时间"、"失效时间"



#### 设置"授权命令配置"-"shell profile配置"

HBC Intelligent Management Center		850 90 <b>0</b>	用户 业务	69	RA NKTE	
用户管理	>	A用户>设备用户保助管理>	● 地址用户 協 所有用户			
设备用户管理	>	授权命令配置	<ul> <li>用户附加信息</li> <li>用户时加信息</li> </ul>			
设备用户策略管理	*	52	▲ 导入用户 ▲ 铁号群巡管理		2	
- 慶 快速入门 - 马 授权策略管理		Shell Profile	设备用户管理 设备用户预用管理 来实法入管理			
• 授权场置条件					接受活要条件 1952年3月21日	Shell Profile
· 12000~~ 2200 - 予 1244世纪					日本の学校の目的では、 したので、 したのので、 したので、 したので、 したので、 したのので、 したのので、 したのので、 したので、 しので、 しのので、 しのので、 しの	76 STREET
<ul> <li>LDAP业务管理</li> <li>业务参救配置</li> </ul>						
来直接入管理	>					

设置"shell profile名称"-"授权级别"

用户管理	>	%用户 > 设备用户策略管理 >	授权命令配置 > Shell Profile	配置 > 堆加Shell Pro	ofile
设备用户管理	>	地加Shell Profile			
设备用户策略管理	~	Shell Profile名称*	H3C V7-15		
展 快速入门		输入控制列表			1
马,授权策略管理		授权规则	15		
• 授权场景条件		间面时长			分钟
• 授权命令配置		会话时长			<del>2)10</del>
· 罗 说着管理		自动执行命令			
▶ LDAP业务管理		自定义履性	Whalietz 🕐		
• 业务参数配置		描述			
來其接入管理	>				

### 设置"命令集配置"

H3C Management Center		1107 <b>902</b> 0	RP 485	8.99	服务 系统管理	
についていたい     にのい     についていたい     にのい     にのい	~ ~ ~	11時 第20     12時     12時	田子 (1)方 田の町二 松田市 田の町二 田の町にの高市 田の町にの高市 田の町にの高市 田の町に町面 松田の市町面 松田の市町面 松田の市町面 田田 田 田田 田 田田 田田 田田 田田 田田 田田 田 田 田田 田田 田田 田 田 田田 1 1	55/35 >	(2条 系統社会) (法入公(約5)(余 0) (注)(法入)(2)(5)(5)(5)(5)(5)(5)(5)(5)(5)(5)(5)(5)(5)	ព៌លិសភ្លេចទ ៖
<ul> <li>         ・</li></ul>					時代的心和28 う 記名面示 LDAP出身常確 业分争的配置	▶ 5 <u>3 Shell Profile</u> 器器 ⑤ 田中県創業
<b>宋<b>庆</b>接入繁建</b>	>					

设置"命令集名称"、"缺省授权方式"



### 配置"设备管理"

HBC Intelligent Management Center		1100 9000	用户	165	69	IEA	55619 <b>1</b>	
电中管理	>	· · · · · · · · · · · · · · · · · · ·	12 > 10 加加用中 12 > 10 所有用中					
24年月中管理	>	titta Ristri	副用户附加 基用户附加	188				
24月户外的管理	v		· 导入用中					
- 周 快速入门		命令集名称 🔺	200 E 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	11121年 1111日				
B. 4047000000788		H3C V7	26/8/10/190	682	•	₹ 1988,207		
· · · · · · · · · · · · · · · · · · ·		共有1条记录。	来宾接入管	e.	•	马 派权用地管理	±	
• 按权场量低件						561X101809014		
▶ 授权命令配置						· 记录管理	)	
· 学 设备管理						业务学数配置		:
▶ LDAP业务管理								
• 业务参数配置								
和再接入管理	>							

增加设备,设置"共享密钥"、"确认共享密钥",绑定"设备区域"、"设备类型"

		na	930	和P	98	8.9	IRA	8566821W	
电户管理	>	B RP > RMRP	MINE I	> 说你做理 > 1	8301R46				
2备用户管理	>	设备配置							
设备用户单路管理	×	共享密明*					1		
- 覆 快速入门		确认共享密闭。					1		
· B. 拉松神醉怪理		以运输口 •		49			T		
授权场景条件		设备区域		内网络心说	5		四百		
授权命令配置		设备类型		H3C-V7			16		
₿ 12₩###		前一连续。		不支持					
LDAP业务管理		Watchdog根d		不觉持		•			
业务参数配置		履送							
均益指入管理	>								
		设备管理							
		2271 - 1	F.I.Who	22550	♥ 現示	: TAM不变持	IPv6tett,		
		设备名称				REALPH	thê:		设备型号
		-	-			-			-
		共有1条记录。							

HBC Internet	atini maa	80° 985 81			
地中繁殖		- 设备管理			
09/0-818	, 西闲设备				
公共中一年時世後	· iBelPretz M.	10.190.9.210			10.190.9.210
- 間 快速入门 - 時, 地名阿里里福 - 間の消費条件 - 間のか今般演	2984 9960		면 속	0242	
- 予 必要管理 - LDAP <u>+</u>	·····································	2010 1220000 12200000 120	Participation 副部型符	845204	设备关型
• <u>****5</u>	10.190.9.210	10.190.9.210	ICMP		H3C-V7
果实接入管理	共有1条记录,当前第1-	1,第1/1页。			

设置"设备用户管理"-"所有设备用户"

Management Center		ri ya	·	picas	HU-	169	-	likat	SUMERY	
用户管理	>	£1 用户 > 15	2番用户	管理 > 设计	<b>新用户分组 &gt;</b> :	增加设备用户分	948			
设备用户管理	v	增加设备用	股中分组	8						
▲ 设备用户分组		分组织	分退名称*		НЗС	H3C V7				
₩ 所有设备用户	>>>	授权策略			НЗС	H3C V7				
<b>弘</b> 所有在追用户	>>>	92 <del>531</del>	旧名称							
<ul> <li>         ·</li></ul>		描述								
& LDAP用户管理	>>>	可以管理。	5.57 (BB)	的制作员						
设备用户策略管理	>		-				1000-02.4	-		
来庆烺入管理	>		awn	1002084			1911 (2) 2	FF		ELECON
			adr	nin			admin			THE R
		<b>N</b>	wei	jianing			weijianir	g		管理员
		共有2条	. <b>\$</b> 51							
										462 635

配置"用户设备分组",设置"分组名称"-"授权策略"

印度語	2	時,用户 > 设备用户预赔管理 >	受权策略管理 > 增加授权策略							
8番用户管理	2	授权策略信息								
社会用户策略管理	~	基本信息	🕒 堆加接入授权信息 - Google Chrome							
<ul> <li>● 快速入门</li> <li>● 投税策略管理</li> </ul>		授权策略名。 强武	② 10.190.8.7.8080/imc/tam/authpolicy/addAccessAuthorizeInfo.xhtml 論入授祝信題							
授权场置条件 授权命令配置		□ <sup>启用RSA</sup> 接入授权信息	设备区域	内网核心设备		9 G				
● 设备管理 LDAP业务管理		Mitto 12MIXHE	设备类型	H3C-V7 工作時前间	•	16				
业务学数配置		不限	Shell Profile	H3C V7-15	•					
实谅入管理	>		授权命令集	H3C V7	٣					
				<b>10</b> 0	808					

绑完"设条区域"-"设备类型"-"授权时段"-"shell profile"-"授权命令集"

		11588 0576	2. monto					
もの管理	>	5 用户 > 设备用户策略管理	2 A KAR					
设备用户管理	>	操作结果	用户附加	LOR. LAT				
设备用户策略管理	~	操作结果		198		取1个,失败	0个。	
辰 快速入门			设备用户管理					
B. 10172984899780			设备用户加电	1970	٠	■ 快速入门		
- CELONDERIE			朱直接入管理		•	<ul> <li>NetX House</li> </ul>	25	
• 授权场服条件						展权场景杂州		•
网络白山山田田						接权命令配置		•
CONTRACTOR .						D SHEE	_	
5 设备管理						LUAP (29) IES	*	
▶ LDAP业务管理						100 PRABLE		
业务学校起置								
积实接入管理	>							

配置"授权管理"

HBC Intelligent Management Center		首页	1000	RP	1695	88	1EA	
用户管理	>	▲用户 > 设备用户	中管理 > 设备	記 増加用户 (図)所有用户				
设备用户管理	~		1842 849	利用中的tora	8			
且 设备用户分组			atorea	45 用户就建筑 是 导入用户	15			
★ 所有设备用户	>>>	分加名称		设备用户管理	-1	•	A (048800	HE CONTRACTOR
<b>弘</b> 所有在线用户	>>>	H3C V7		设备用户策结常 床直速入管理	<b>全理</b>	:	· 二 新有設備用 私)新用用 また	
劉 累名弟用户		未分担					1 第名单用户	1
<ul> <li>日志堂理</li> </ul>							日本管理	erce.
& LDAP用户管理	>>>						Ch county i	
设备用户策略管理	>							
来直接入管理	,							

设置"账号名"-"登陆密码"-"登陆密码确认"-"设备用户分组"-"用户的授权策略"

APPERD         3         MUNDPROVEND VERSIONEND VERSIONEND VERSIONEND           Aussimmet         VERSION         VERSION           Basemet	HBC Internet		#10 MIN	80 95			SISTE			
▲ 0.800/m/00         N/6 / animal           ▲ 0.000/m/00         Animal           ▲ 0.	用い数理 IOM/Dの数理	÷ v	安市。> 15年前小田田 > 15年 1820256月10	nice aller > Herochert	lo.					
CARAD-WRIET         CARAD-WRIET	акат-рад акат-рад - Сторьяй - Сторьяй - Сторьяй - Какатан- - Какатан- - Какатан- - Какатан-	209 319 329	相母名。 登录者員。 公司前の分明。 分司的世代年期 公司前期前期	admintacaes HBC V7 HBC V7 255 Websellity: 1 th	1255 2.84.	Ø		ID=45 Strestanu - Ru=5255748	admintacaes HIJC V7	•
[전도] 학교가 5년 위원 전문 1800년 1810년 1820년 1841년 1811년 18			105- 105- 106-00087-007	ULThing://WC1服務	Bittl:port/inc/	noAuth/lum/	login.jul			
et 80			授权主机IPR5法列表 1008 898-59 8089903 #0599768440020。					NUG SPYINZ 102 001		

S1850 hwtacacs配置如下:

hwtacacs scheme shebeiguanli primary authentication 10.190.8.7 primary authorization 10.190.8.7 primary accounting 10.190.8.7 key authentication nnhwtacacs key authorization nnhwtacacs key accounting nnhwtacacs user-name-format without-domain nas-ip 10.190.9.210 quit

domain tamdm

authentication login hwtacacs-scheme shebeiguanli local authorization login hwtacacs-scheme shebeiguanli local accounting login hwtacacs-scheme shebeiguanli local authorization command hwtacacs-scheme shebeiguanli local accounting optional quit

local-user admin password simple admin service-type terminal ssh quit

user-interface vty 0 15 authentication-mode scheme command accounting command authorization

#### 查看hwtacacs状态:

#### dis hwtacacs

HWTACACS-server templa	ate name	e : shebeiguanli
Primary-authentication-ser	ver :1	0.190.8.7:49
Primary-authorization-serv	er :10	0.190.8.7:49
Primary-accounting-server	: 1(	0.190.8.7:49
Secondary-authentication-	server :	0.0.0.0:0
Secondary-authorization-s	erver :	0.0.0.0:0
Secondary-accounting-ser	ver :	0.0.0.0:0
Current-authentication-ser	ver :1	0.190.8.7:49
Current-authorization-serve	er :10	0.190.8.7:49
Current-accounting-server	: 10	).190.8.7:49
Nas-IP address	: 10.19	0.9.210
key authentication	. *****	
key authorization	. *****	
key accounting	. *****	
Nas-IP address	: 10.19	0.9.210
Quiet-interval(min)	: 5	
Realtime-accounting-interv	al(min) :	12
Response-timeout-interval	(sec) :	5
Acct-stop-PKT retransmit t	imes :	100
Username format	: with	out-domain
Data traffic-unit :	В	
Packet traffic-unit	: one-pa	cket

Total 1 HWTACACS scheme(s).

#### 查看domain的显示信息:

dis domain tamdm Domain: tamdm State: Active Access-limit: Disabled Accounting method: Optional Default authentication scheme : local Default authorization scheme : local Default accounting scheme : local Login authentication scheme : hwtacacs:shebeiguanli, local Login authorization scheme : hwtacacs:shebeiguanli, local Login accounting scheme : hwtacacs:shebeiguanli, local : hwtacacs:shebeiguanli, local Command authorization scheme Domain User Template: Idle-cut : Disabled Self-service : Disabled Authorization attributes:

---

至此, S1850交换机hwtacacs典型组网配置案例已完成!