# 使用Active Directory和RV34x路由器的远程身份 验证和登录指南

## 目标

本文介绍如何在Cisco RV34x系列路由器上使用Windows Active Directory(AD)配置远程身份验证。 此外,还将提供信息以避免潜在的登录错误。

## 简介

在RV34x路由器上配置服务身份验证设置时,需要选择外部身份验证方法。

默认情况下,RV34x系列路由器上的外部数据库优先级为RADIUS/LDAP/AD/Local。如果在路由器 上添加RADIUS服务器,Web登录服务和其他服务将使用RADIUS外部数据库对用户进行身份验证 。没有为Web登录服务单独启用外部数据库并为其他服务配置其他数据库的选项。在路由器上创建 并启用RADIUS后,路由器将使用RADIUS服务作为外部数据库进行Web登录、站点到站点VPN、 EzVPN/第三方VPN、SSL VPN、PPTP/L2TP VPN和802.1x。

如果使用Windows,Microsoft提供内部AD服务。AD存储网络的所有基本信息,包括用户、设备和 策略。管理员将AD用作创建和管理网络的单一位置。它便于以统一方式处理互联、复杂和不同的网 络资源。

配置后,任何获得授权的人都可以使用外部AD选项(存在于Windows服务器操作系统中)进行身份 验证,以在RV34x路由器上使用任何特定服务。授权用户可以使用所提供的功能,只要他们拥有使 用此类身份验证所需的硬件和软件。

#### 适用设备 |软件版本

- RV340 |1.0.03.16
- RV340W |1.0.03.16
- RV345 |1.0.03.16
- RV345P |1.0.03.16

#### 目录

- 确定可分辨名称值
- <u>为Active Directory创建用户组</u>
- 在RV34x路由器上添加Active Directory详细信息
- 如果不从全名字段中取出空格,会发生什么情况?

# 确定可分辨名称值

访问Windows *2016服务器上*的Active Directory用户和计算机管理界面。选择"用**户"**容器文件夹,右 键单击鼠标,然后打开"属**性"**。请注意稍后将*在RV34x路*由器用户容器路径字段中*使用的 DistinguishedName*值。

File Action Media Clipboard View Help	
🗄   💿 💿 🥥   💵 🕨   💺 5   🗮	
Active Directory Users and Computers	
Re File Action View Help	
← ⇒   2 📷   4 🗉   🗙 🗟 0 🕞   🛛 🖬   🐍 📚 🗑 🍸 🗕 🗞	
Active Directory Users and Computers [sb Name	Type
> 📫 Saved Queries 🌼 👘 👘 👘 👘 👘 👘	

# 为Active Directory创建用户组

### 第1步

登录RV34x系列路由器。导航至**系统配置>用户组**。



### 步骤 2

#### 单击加号**图标**。



### 步骤 3

输入组名称。单击 Apply。

CISCO RV345P-RV345P	English 🔻 😯 🚺 🕩
User Groups	2 Apply Cancel
Overview Group Name: RemoteAdmin	

在本示例中,已创建了RemoteAdmin用户组。

点击新用户组旁边的复选框。单击编**辑图标**。



向下滚动页面至"服务"。单击"Administrator(管理员)"单选按钮。

Services
Web Login/NETCONF/RESTCONF O Disabled O Read Only O Administrator Site to Site VPN
步骤 6
单击 Apply。
Apply Cancel
步骤 7

您现在将看到显示具有管理员权限的新用户组。

			cisco R	V345P-router4491EF				cisco (admir	Englist		
⊗ •	Getting Started Status and Statistics	U	ser Groups						Ap	oply Ca	ancel
	Administration	ı	Jser Groups Table								^
•	System Configuration		+ 🕜 🛍								
	System		Group 🗢	Web Login/NETCONF/RESTCONF \$	S2S-VPN \$	EzVPN/3rd Party 🗢	SSL VPN \$	PPTP \$	L2TP 🗢	802.1x 🖨	
	System Time	(	<ul><li>□ Group ≑</li><li>□ RemoteAdmin</li></ul>	Web Login/NETCONF/RESTCONF +	S2S-VPN \$	EzVPN/3rd Party \$	SSL VPN \$	PPTP <b>≑</b> Disabled	L2TP \$ Disabled	802.1x ¢	_
	System Time Log	(	<ul> <li>Group \$</li> <li>RemoteAdmin</li> <li>admin</li> </ul>	Web Login/NETCONF/RESTCONF & Admin Admin	S2S-VPN \$ Disabled Disabled	EzVPN/3rd Party Disabled Disabled	SSL VPN \$	PPTP 🗢 Disabled Enabled	L2TP 🗢 Disabled Enabled	802.1x ¢ Disabled Enabled	
	System Time Log Email	(	<ul> <li>Group \$</li> <li>RemoteAdmin</li> <li>admin</li> <li>anyconnect</li> </ul>	Web Login/NETCONF/RESTCONF \$ Admin Admin Disabled	S2S-VPN \$ Disabled Disabled Disabled	EzVPN/3rd Party \$ Disabled Disabled Disabled	SSL VPN \$ Disabled SSLVPNDef	PPTP 🗢 Disabled Enabled Disabled	L2TP \$ Disabled Enabled Disabled	802.1x \$ Disabled Enabled Disabled	
	System Time Log Email User Accounts	(	<ul> <li>Group \$</li> <li>RemoteAdmin</li> <li>admin</li> <li>anyconnect</li> <li>guest</li> </ul>	Web Login/NETCONF/RESTCONF \$ Admin Admin Disabled Disabled	S2S-VPN \$ Disabled Disabled Disabled Disabled	EzVPN/3rd Party \$ Disabled Disabled Disabled Disabled	SSL VPN \$ Disabled SSLVPNDef SSLVPNDef Disabled	PPTP \$ Disabled Enabled Disabled Disabled	L2TP \$ Disabled Enabled Disabled Disabled	802.1x ¢ Disabled Enabled Disabled Disabled	

# 在RV34x路由器上添加Active Directory详细信息

#### 第1步

导航到**系统配置>用户帐户。**选择AD选项,然后单**击编**辑图标以添加AD服务器的详细信息。

		😆 ''	lili. cisco	RV345P-route	er4491EF			cisco (admin)	English	• ?	<b>()</b> ()
$\otimes$	Getting Started	l Iser A	ccour	nts						anly	Cancel
•	Status and Statistics	00017	00000	110					A	opiy	Cancer
**	Administration	* Should ha	ave at leas	st one account in t	he "admin" g	group					
<b>¢</b> (	System Configuration				<u> </u>						
	System 1	Remot	e Auti	nentication	Service	2					
	Time	Remote	Authentic	cation Service Ta	ble						^
	Log	4+0									
	Email	🗆 Ena	able 🗢	Name 🕈		Primary Server \$	Back	up Server 🗢			
	User Accounts 2			AD 3							
	User Groups	0 0		LDAP							
	IP Address Groups	0 0		RADIUS							
	SNMP										
	Discovery-Bonjour	* Please inp	out remote	e authentication se	ervice configu	rations when it is enabled.					

#### 步骤 2

输入AD域名、主服务器、端口和用户容器路径详细信息。单击 Apply。

	RV345P-router4491EF	cisco (RemoteAdmin) English 🕤 ? 🚺 🖨
User Accou	nts	Apply Cancel
Add/Edit Ne	w Domain	
Name	AD	
Authentication Type	Active Directory	
Authentication Type	Active Directory sbcslab.local	
Authentication Type AD Domain Name Primary Server	Active Directory sbcslab.local 172.16.1.2 Port 389	

**注意:**您需要在本文的"识*别可分辨名*称值"部分输入从Windows服<u>务器捕获的用户容</u>器路径详细信 息。

在本例中,详细信息*为Cn=user,dc=sbcslab,dc=local*。轻量级目录访问协议(LDAP)服务器默认 侦听端口为389。

#### 步骤 3

在AD中,验证用户组*是否已*配置,并且它与路由器的用户组名称匹配。

FI	e Action Media Clipboard View Help			
8	a   🕲 💿 🕲 😫 💷 🕨   陸 🕒   🖳			
٦	<ul> <li>Active Directory Users and Computers</li> <li>File Action View Help</li> <li>File I 2 III X III N III IIII</li> </ul>	a 1 🐮 🐮 🗃 🍸 🚨 🔽	_	×
	<ul> <li>Active Directory Users and Computers [sbcslabfores</li> <li>Saved Queries</li> <li>sbcslab.local</li> <li>Builtin</li> <li>Computers</li> <li>Domain Controllers</li> <li>Saved Computers</li> </ul>	Name Reterprise Read-only Domain Controllers Group Policy Creator Owners Guest Key Admins Key Keyt	Type Security Group - Universal Security Group - Global User Security Group - Global User	

在"新对象 — 用户"下,填写"名"、"名"、"姓"和"姓","全名"字段将自动填充,其中显示名和姓之间的 空格。

必须删除"全名"框中名字和*姓氏*之间的空格,否则无法正确登录。

此图显示必须删除的全名中的空间:

File Action Media Clipboard View Help		
🗄 🕘 🖲 🔕 😒 💷 🕩 🔂 🗉	2	
Active Directory Users and Computers		
File Action View Help		
File     Action     View     Help       Image: Active Directory Users and Computers [sb     Image: Active Directory Users and Computers [sb       Image: Active Directory Users and Computers [sb       Image: Active Directory Users and Computers [sb       Image: Active Directory Users and Computers [sb       Image: Active Directory Users and Computers [sb       Image: Active Directory Users and Computers [sb       Image: Active Directory Users and Computers [sb       Image: Active Directory Users and Computers [sb       Image: Active Directory Users and Computers [sb       Image: Active Directory Users and Computers [sb       Image: Active Directory Users and Computers [sb       Image: Active Directory Users and Computers [sb       Image: Active Directory Users and Computers [sb       Image: Active Directory Users and Computers [sb       Image: Active Directory Users and Computers [sb       Image: Active Directory Users and Computers [sb       Image: Active Directory Users and Computers [sb       Image: Active Directory Users and Computers [sb       Image: Active Directory Users [sb       Image: Active	Image: Solution of the second seco	Type Security Group - Global Security Group - Global X x sbcslab.local/Users ad Initials: 2
	Guest     G	e-Windows 2000): 4 edadmin 5 Cancel User

### 步骤 5

重复上述步骤以创建其他用户。再次,您需要通过删除自动创*建的空*格来修改"全名"字段。单击 Next设置密码并完成用户创建。

此图显示"全名"中的空间已删除。这是添加用户的正确方法:

File Action Media Clipboard View Help		
🗄 🕘 🖲 🥥 🖸 💷 🕒 🗒		
Active Directory Users and Computers		
File Action View Help		
🔶 🔶 📶 🐇 🗙 🗊 🕞 📓 🕫	1 😤 📚 🛍 🍸 🧕 📚	
<ul> <li>Active Directory Users and Computers [sb</li> <li>Saved Queries</li> <li>Subcslab.local</li> <li>Builtin</li> <li>Computers</li> <li>Domain Controllers</li> <li>ForeignSecurityPrincipals</li> <li>Keys</li> <li>LostAndFound</li> <li>Managed Service Accounts</li> <li>Program Data</li> <li>System</li> <li>Users</li> <li>NTDS Quotas</li> <li>TPM Devices</li> </ul>	Name New Object - User RemoteA Enterprise Enterprise Schema A Admin Us Admin Us Admin Us Admin Us AdminiUs Admini AdminiUs Admini	Initials:
	User 2 User	

"用户"(Users)列表将显示两个新添加的用户详细信息。

File Action Media Clipboard View Help		
🖦   🕘 💿 🥥   🖬 🕩   🔂 🍮		
Active Directory Users and Computers		
File Action View Help		
le →   2 📰   🔏   🗙 🗟 🔒   🛛 🗉	i 🗏 🔽 📷 🔻 🗾 🐍	
<ul> <li>Active Directory Users and Computers [sb</li> <li>Saved Queries</li> <li>Saved Queries</li> <li>Substab.local</li> <li>Builtin</li> <li>Computers</li> <li>Domain Controllers</li> <li>ForeignSecurityPrincipals</li> <li>Keys</li> <li>LostAndFound</li> <li>Managed Service Accounts</li> <li>Program Data</li> <li>System</li> <li>Users</li> <li>NTDS Quotas</li> <li>TPM Devices</li> </ul>	Name Enterprise Admins Enterprise Key Admins Enterprise Key Admins Enterprise Read-only Domain Controllers Schema Admins Admin User2 Admin User3 Admin User3 AdminUser3 AdminUser4 AdminUser0 AdminUser1 DefaultAccount Guest krbtgt L2TP User1 PPTP User1 PPTP User1 PPTP User1 PPTP User1 SBCS admin SBCS admin Sbcs labadmin1 User 0 User 0 User 0	Type Security Group - Universal Security Group - Universal Security Group - Universal Security Group - Universal User User User User User User User User
	User 1 User 2 User 3	User User User
	👗 User 4	User
	Subser 5	User
	Suser 6	User
	Subser /	User
	💍 User 8	User
	A declaring	User
	💿 ad admin i	User
< >	auadminz	oser

#### 步骤 7

您会注意到,ad admin1显示名字和姓氏之间的空格,如果这不是固定的,登录将失败。此错误留 在演示中,请勿留空间!adadmin2示例正确。

要查看,请右键单击ad admin 1*用户名,*然后选择"属**性"**选项。然后导航至"对**象"**选项卡,查看"对 *象"详细信息的规范*名称。

ad admin1 Prop	erties		? ×	Si Si	adadmin2 Prop	erties		? ×
Security Remote Des	Environment ktop Services Profile	Sessions COM+	Remote control Attribute Editor	U U	Security Remote Des	Environment sktop Services Profile	Sessions COM+	Remote control Attribute Editor
General Ac Published Certifi Canonical nam sbcslab.local/	ddress Account cates Member Of e of object: Users/ad admin1	Profile Telep Password Replica	hones Organization ation Dial-in Object	U U U U	General Ac Published Certifi Canonical nam sbcslab.local/	ddress Account icates Member Of ee of object: /Users/adadmin2	Profile Telepi Password Replica	hones Organization ation Dial-in Object
Object class:	User			U	Object class:	User		

此外,您还可以导航至"属性"*选项下的"成员"*选项卡,以验证这些用户名的"域用户"和*远程管理*详细 信息。



#### 导航至属性编辑器选项卡,以验证这些用户名的DistinguishedName值。

Security	Environment	Sess	ions	Remote co	ontrol	U Se	curity	E	nvironment	Sessi	ions F	Remote co	ontrol
General Address	s Account	Profile	Telephon	ies Organ	nization	U Gene	ral	Address	Account	Profile	Telephones	Orga	nizati
blished Certificates	Member Of	Password	d Replication	n Dial-in	Object	U Publis	hed C	ertificates	Member Of	Password	Replication	Dial-in	ОЫ
Remote Desktop	Services Profile	CC	DM+	Attribute E	ditor	U Re	mote	Desktop S	ervices Profile	CC	DM+	Attribute E	Editor
Attributes:						U Attrib	utes:						
ibute	Value				^	U tribu	te		Value				^
partmentNumber	<not set=""></not>					U sfault	Class!	Store	<not set=""></not>				
cription	<not set=""></not>					u spart	ment		<not set=""></not>				
ktopProfile	<not set=""></not>					- part	mentN	umber	<not set=""></not>				
tinationIndicator	<not set=""></not>					u escrip	otion		<not set=""></not>				
olayName	ad admin1					eskto	oProfi	le	<not set=""></not>				
						- Distance	P						
playNamePrintable	<not set=""></not>					U estina	tionIn	dicator	<not set=""></not>				
olayNamePrintable inguishedName	<not set=""> CN=ad admi</not>	n1,CN=Use	ers,DC=sbcs	lab,DC=loca		U estina U splay	, ationIn Name	dicator	<not set=""> adadmin2</not>				
playNamePrintable tinguishedName	<not set=""> CN=ad admir that add</not>	n1,CN=Use	ers,DC=sbcs	lab,DC=loca		U estina U splay U splay	ationIn Name Name	dicator Printable	<not set=""> adadmin2 <not set=""></not></not>				
ilayNamePrintable inguishedName  Signature	<not set=""> CN=ad admin that add set&gt;</not>	n1,CN=Use	ers,DC=sbcs	lab,DC=loca	ו	U solav U splay U solav U sting	ationIn Name Name uisheo	dicator Printable Name	<not set=""> adadmin2 <not set=""> CN=adadmin</not></not>	2,CN=Use	rs,DC=sbcslab	),DC=loca	ł
layNamePrintable nguishedName  Signature CorePropagationD	<not set=""> CN=ad admin (not oot) <not set="">  0x0 = ( )</not></not>	n1,CN=Use	ers,DC=sbcs	lab,DC=loca		U splay U splay U splay U sting	ationIn Name Name uisheo	dicator Printable Name	<not set=""> adadmin2 <not set=""> CN=adadmin</not></not>	2,CN=Use	rs,DC=sbcslab	),DC=loca	1
NayNamePrintable InguishedName Jon Signature CorePropagationD amicLDAPServer	<not set=""> CN=ad admit (not set&gt; (not set&gt; 0x0 = () (not set&gt;</not>	n1,CN=Use	ers,DC=sbcs	lab,DC=loca		U splay U splay U splay U sting U vision	ationIn Name Name uisheo gnatur	dicator Printable IName e	<not set=""> adadmin2 <not set=""> CN=adadmin <not set=""> <not set=""></not></not></not></not>	2,CN=Use	rs,DC=sbcslab	),DC=loca	1
olayNamePrintable inguishedName Signature CorePropagationD IamicLDAPServer ployeeID	<not set=""> CN=ad admin that cols <not set="">  0x0 = ( ) <not set=""> <not set=""></not></not></not></not>	n1,CN=Use	ers,DC=sbcs	lab,DC=loca		U solay U splay U solay U sting U vision U SASin	ation In Name Name uisheo gnatur ePropa	dicator Printable IName e agationD	<not set=""> adadmin2 <not set=""> CN=adadmin <not set=""> (not set&gt; 0x0 = ( )</not></not></not>	2,CN=Use	rs,DC=sbcslab	),DC=loca	ł
olayNamePrintable inguishedName ASignature CorePropagationD namicLDAPServer ployeeID ployeeNumber	<not set=""> CN=ad admit that sets <not sets<br=""> 0x0 = ( ) <not sets<br=""><not sets<br=""><not sets<="" td=""><td>n1,CN=Use</td><td>ers,DC=sbcs</td><td>lab,DC=loca</td><td></td><td>U solay U solay U solay U sting U vision U SASin U SCon</td><td>ationIn Name Name uished gnatur ePropa</td><td>dicator Printable IName e agationD PServer</td><td><not set=""> adadmin2 <not set=""> CN=adadmin <not set=""> 0x0 = ( ) <not set=""></not></not></not></not></td><td>2,CN=Use</td><td>rs,DC=sbcslab</td><td>),DC=loca</td><td>1</td></not></not></not></not></not>	n1,CN=Use	ers,DC=sbcs	lab,DC=loca		U solay U solay U solay U sting U vision U SASin U SCon	ationIn Name Name uished gnatur ePropa	dicator Printable IName e agationD PServer	<not set=""> adadmin2 <not set=""> CN=adadmin <not set=""> 0x0 = ( ) <not set=""></not></not></not></not>	2,CN=Use	rs,DC=sbcslab	),DC=loca	1
playNamePrintable tinguishedName isies. ASignature CorePropagationD namicLDAPServer ployeeID ployeeID ployeeNumber ployeeType	<not set=""> CN=ad admit (not set) (not set) (not set) (not set) (not set) (not set) (not set)</not>	n1,CN=Use	ers,DC=sbcs	lab,DC=loca	Ŭ,	U solar U splay U splay U sting U vision U SASin U Corr U nam	ationIn Name Name uished gnatur eProp icLDA veeID	dicator Printable IName e agationD PServer	<pre><not set=""> adadmin2 <not set=""> CN=adadmin CN=adadmin Cnot set&gt; CN=adadmin Cnot set&gt; Ox0 = ( ) <not set=""> <not set=""> <not set=""> </not></not></not></not></not></pre>	2,CN=Use	rs,DC=sbcslab	),DC=loca	4

#### 步骤 8

使用用户登录名登录,在本例中为adadmin2,您将看到登录成功。

#### 步骤 9

#### 您可以查看数据包捕获的详细信息,如以下屏幕截图所示。

💰 Capturing from Ethernet	_		×
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help			
📶 📕 🧶 🐵 📄 🖄 🖾 🔍 🗢 🗢 🕾 😨 🕭 🚍 🔄 Q. Q. Q. X			
📕 ldəp	- Expr	ession	. +
No. Time Source Destination Protocol Lengt Info			^
2097 231.107_ 172.16.1.2 172.16.1.126 LDAP 220 searchResDone(2) noSuchObject (0000208D: NameErr: DSID-03100241, problem 2001 (NO_06JECT), dat	a 0, b	est ma	at_
2851 329.849_ 172.16.1.126 172.16.1.2 LDAP 99 bindRequest(1) "adadmin2@SBCSLAB.LOCAL" simple			1
2852 329.883_ 172.16.1.2 172.16.1.126 LDAP 76 bindResponse(1) success			
2854 329.883_ 172.16.1.126 172.16.1.2 LDAP 143 searchRequest(2) "cn=adadmin2,cn=Users,dc=sbcslab,dc=local" wholeSubtree			
2855 329.896_ 172.16.1.2 172.16.1.126 LDAP 206 searchResEntry(2) "CN=adadmin2,CN=Users,DC=sbcslab,DC=local"   searchResDone(2) success [1 r	esult]		
2856 329.897_ 172.16.1.126 172.16.1.2 LDAP 61 unbindRequest(3)			
			~
<pre>&gt; Frame 2855: 206 bytes on wire (1648 bits), 206 bytes captured (1648 bits) on interface 0 &gt; Ethernet II, Src: Microsof_01:7e:01 (00:15:5d:01:7e:01), Dst: Cisco_44:57:7f (ec:bd:1d:44:57:7f) &gt; Internet Protocol Version 4, Src: 172.16.1.2, Dst: 172.16.1.126 &gt; Transmission Control Protocol, Src Port: 389, Dst Port: 59096, Seq: 23, Ack: 135, Len: 152 &gt; Lightweight Directory Access Protocol &gt; LDAPMessage searchResEntry(2) "CN=adadmin2,CN=USers,DC=sbcslab,DC=local" [1 result] &gt; LDAPMessage searchResDone(2) success [1 result]</pre>			

# 如果不从全名字段中取出空格,会发生什么情况?

如果尝试使用*用户登录名*,在本例中为*adadmin*,则会看到登录失败,因为轻量目录访问协议 (LDAP)服务器无法返回对象,因为*全名*(在本例中为*adadmin1,*)有空格。您将能够在捕获数据包时 看到详细信息,如以下屏幕截图所示。

# 结论

您现在已成功完成并避免了通过RV34x路由器上的Active Directory进行远程身份验证的失败登录。