# 使用Active Directory和RV34x路由器的遠端身份 驗證和登入指南

## 目標

本文說明了如何在Cisco RV34x系列路由器上使用Windows Active Directory(AD)配置遠端身份驗證 。此外,還會提供資訊,以避免潛在的登入錯誤。

## 簡介

在RV34x路由器上配置服務身份驗證設定時,需要選擇外部身份驗證方法。

預設情況下,RV34x系列路由器上的外部資料庫優先順序為RADIUS/LDAP/AD/Local。如果在路由 器上新增RADIUS伺服器,Web登入服務和其他服務將使用RADIUS外部資料庫驗證使用者。沒有 選項可以單獨為Web登入服務啟用外部資料庫並為其他服務配置另一個資料庫。在路由器上建立並 啟用RADIUS後,路由器將使用RADIUS服務作為Web登入、站點到站點VPN、EzVPN/第三方 VPN、SSL VPN、PPTP/L2TP VPN和802.1x的外部資料庫。

如果您使用Windows,Microsoft會提供內部AD服務。AD儲存網路的所有基本資訊,包括使用者、 裝置和策略。管理員使用AD作為單一位置建立和管理網路。它有助於以統一的方式處理互連、複雜 和不同的網路資源。

配置後,任何獲得授權的使用者都可以使用外部AD選項(在Windows伺服器作業系統中)進行身份 驗證,以使用RV34x路由器上的任何特定服務。授權使用者可以使用提供的功能,只要他們擁有使 用該型別身份驗證所需的硬體和軟體。

#### 適用裝置 |軟體版本

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

#### 目錄

- 標識可分辨名稱值
- 為Active Directory建立使用者組
- 在RV34x路由器上新增Active Directory詳細資訊
- 如果不從全名欄位中取出空格會發生什麼?

## 標識可分辨名稱值

訪問Windows 2016伺服器上的Active Directory使用者和電腦管理介面。選擇**Users**容器資料夾,按 一下右鍵滑鼠,然後開啟**Properties**。請注意稍後將在RV34x路由器*User Container Path*欄位中使 用的*DistinguishedName*值。

File Action Media Clipboard View Help	
🖴   💿 💿 🥥   💵 🕨   🛼 🖕   🗮	
Active Directory Users and Computers	
R, File Action View Help	
← ⇒ 2 m 4 1 × 0 0 ≥ 1 ∞ 1 × 0 7 2 ×	
Active Directory Users and Computers [sb Name	Type
Saved Queries	

## 為Active Directory建立使用者組

### 步驟1

登入到RV34x系列路由器。導覽至System Configuration > User Groups。



### 步驟2

#### 點選加**號圖示**。



## 步驟3

輸入組*名稱*。按一下「Apply」。

E CISCO RV345P-RV345P	English 🔹 😮 🚺 🕩
User Groups	2 Apply Cancel
Overview Group Name: RemoteAdmin	

#### 在此示例中,*已創*建了一個RemoteAdmin使用者組。

按一下新使用者組旁邊的覈取方塊。按一下**edit**圖示。



## 在RV34x路由器上新增Active Directory詳細資訊

#### 步驟1

導航到系統配置>使用者帳戶。選擇AD選項並按一下edit icon以新增AD伺服器的詳細資訊。

	CISCO RV345P-router4491EF		💾 cisco (a	idmin) Englist 🔹 😯 🚺 🕩							
	User Accounts			Apply							
🕒 Status and Statistics											
Administration	* Should have at least one account in the " admin" group										
System Configuration	Demote Authentication Comis										
System 1	Remote Authentication Servic	e									
Time	Remote Authentication Service Table			^							
Log	4+12										
Email	□ Enable <b>\$</b> Name <b>\$</b>	Primary Server \$	Backup Server 🗢								
User Accounts 2	✓ AD 3										
User Groups	LDAP										
IP Address Groups	C C RADIUS										
SNMP											
Discovery-Bonjour	* Please input remote authentication service config	gurations when it is enabled.									

#### 步驟2

輸入AD域名、主伺服器、埠和使用者容器路徑詳細資訊。按一下「Apply」。

	RV345P-router4491EF	cisco (RemoteAdmin) English 🔤 😯 🚺 🕞
User Accou	nts	Apply Cancel
Add/Edit Ne	w Domain	2
N 1		
Name	AD	
Name Authentication Type	AD Active Directory	
Name Authentication Type AD Domain Name	AD Active Directory sbcslab.local	
Name Authentication Type AD Domain Name Primary Server	AD Active Directory sbcslab.local 172.16.1.2 Port 389	0

**附註**:您需要在本文<u>識別可分辨名稱值</u>部分輸入從Windows伺服器捕獲的使用者容器路徑詳細資訊 。

在本示例中,詳細資訊是*Cn=user,dc=sbcslab,dc=local*。輕量型目錄訪問協定(LDAP)伺服器預 設偵聽埠為389。

#### 步驟3

在AD中,驗證是否配置了User Group,並且它匹配路由器的User Group名稱。

File Action Media Clipboard View Help			
🗄   💿 💿 🞯 🔋 🔢 🕩   💺 🗅   🖳			
Active Directory Users and Computers F File Action View Help		_	×
🗢 🔿 🙍 🔣 🖬 🐇 🗎 🔀 🖬	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> </ul>	Name Reference in the interval of the interva	Type Security Group - Universal Security Group - Global User Security Group - Global User	

#### 步驟4

在「新對象 — 使用者」(New Object - User)下,填寫*名、首字母和姓氏*,將自動填充*全名*欄位,顯 示名字和姓氏之間的空格。

*全名*」框中的名字和姓之間的空格必須刪除,否則將無法正確登入。

此圖顯示了必須刪除的完整名稱中的空格:

File Action Media Clipboard Vaw Halp		
≞ 0 • 0 0 11 ► 5 5	2	
Active Directory Users and Computers		
File Action View Help		
File Action View Help File Active Directory Users and Computers [sb Active Directory Users and Computers [sb Saved Queries Builtin Computers Builtin Computers Domain Controllers Foreign SecurityPrincipals Keys LostAndFound Managed Service Accounts Program Data System Users NIDS Quotas TPM Devices	Image: Second	Type Security Group - Global Security Group - Global x in: sbcslab.local/Users ad Initials: 2
	Count of the second secon	(pre-Windows 2000): 4 adadmin 5 Cancel User

#### 步驟5

重複這些步驟以建立另一個使用者。同樣,您需要通過刪除自動建立的任何空格來修改*全名*欄位。 按一下**下一步**設定密碼並完成使用者建立。

此圖顯示「全名」中的空格已被刪除。這是新增使用者的正確方式:

File Action Media Clipboard View Help			
🗄 🕘 🖲 🕘 😋 🖬 🕩 📑 🏷	2		
Active Directory Users and Computers			
File Action View Help			
수 🏟 🙇 📷 🔏 🗙 🗊 🔒 🖬 8	m   % 🔌 îj	i 🔻 🧕 🔽	
<ul> <li>Active Directory Users and Computers [sb</li> <li>Saved Queries</li> <li>Sbcslab.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>MTDS Quotas</li> <li>TPM Devices</li> </ul>	Name RemoteAr RemoteAr Renterprise Enterprise Renter	New Object - User Create in: sbcslab lo First mae: Last name: adadmin2 User logon name: adadmin2 User logon name (pre-Windows 20 SBCSLAB\ min1 admin1	cal/Users  cal/Users  initials:  2  cal/Users  cal/User  cal/User  cal/User  cal/User  cancel  cancel
	揭 User 2		User

### 步驟6

使用者清單將顯示新增的兩個使用者詳細資訊。

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	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
	Current Contraction State Stat	User
	Coser 5	User
	Sterr 7	User
	Licer 8	llear
		llcar
	ad admin1	User
	adadmin2	Liser
< >		

### 第7步

您會注意到,ad admin1顯示名字和姓之間的空格;如果不進行修復,登入將失敗。此錯誤留作演示之用,請勿將空間留在那裡!adadmin2示例正確。

要檢視此檔案,請按一下右鍵ad admin 1使用者名並選擇**Properties**選項。然後導航到**Object**頁籤 ,檢視*Object* details的*規範名稱*資訊。

ad admin1 Prop	erties			?	×	Se Se	adadmin2 P	properties				?	$\times$
Security Remote Des	Sessions Remote control COM+ Attribute Editor			rol tor	U U	Security Remote	E Desktop S	nvironment ervices Profile	Sess	sions OM+	Remote co Attribute E	ontrol ditor	
General Ac Published Certifi Canonical nam sbcslab.local/ Object class:	dress Account cates Member Of e of object: Users/ad admin1 User	Profile T Password Re	elephones plication	Organiz Dial-in 0	ation Ibject		General Published ( Canonical sbcslab.k Object cla	Address Certificates Iname of of ocal/Users/	Account Member Of biect adadmin2	Profile Passwor	Telephone: d Replication	Dial-in	Diject

此外,您還可以導航到*屬性*選項下的*成員*頁籤,驗證這些使用者名稱的*域使用者*和*RemoteAdmin*詳 細資訊。



#### 導航到Attribute Editor選項卡,以驗證這些使用者名稱的DistinguishedName值。

			-	S					
Security Er	vironment	Sessions	Remote control	Security	E	nvironment	Sess	ions F	lemote contr
General Address	Account	Profile Teleph	ones Organization	U General	Address	Account	Profile	Telephones	Organiza
ublished Certificates	Member Of	Password Replica	tion Dial-in Obiect	U Published C	ertificates	Member Of	Passwor	d Replication	Dial-in 0
Remote Desktop Se	ervices Profile	COM+	Attribute Editor	U Remote I	Desktop S	ervices Profile	C	OM+ /	Attribute Edit
Attributes:				U Attributes:					
ribute	Value		^	U tribute		Value			^
partmentNumber	<not set=""></not>			U sfaultClass	Store	<not set=""></not>			
scription	<not set=""></not>			U spartment		<not set=""></not>			
sktopProfile	<not set=""></not>			partmentN	umber	<not set=""></not>			
stinationIndicator	<not set=""></not>			scription		<not set=""></not>			
playName	ad admin1			sktopProfi	le	<not set=""></not>			
playNamePrintable	<not set=""></not>			estinationIn	dicator	<not set=""></not>			
tinguishedName	CN=ad admin	n1,CN=Users,DC=sb	cslab,DC=local	U splayName		adadmin2			
	1101-000				Printable	<not set=""></not>			
ASignature	<not set=""></not>			U stinguished	Name	CN=adadmir	2,CN=Use	ers,DC=sbcslab	,DC=local
CorePropagationD	0x0 = ( )			U		CHOC SEC/			
amicLDAPServer	<not set=""></not>			ASignatur	е	<not set=""></not>			
ployeeID	<not set=""></not>			CoreProp	agationD	0x0 = ( )			
ployeeNumber	<not set=""></not>			namicLDA	PServer	<not set=""></not>			
ploveeTvpe	<not set=""></not>		~			<not set=""></not>			~
<			>	U <					>
Edit			Filter	U Edit					Filter

#### 步驟8

使用User logon name(本例中為adadmin2)登入,您將看到登入成功。

#### 步驟9

您可以看到資料包捕獲的詳細資訊,如下面的螢幕截圖所示。

	Capturing from Ethernet —									
F	ile Edi	t View G	o Capture Ana	lyze Statistics	Telephony	Wireless Tools Help				
4	( 🔳 🖌	I 🖉 @   📄 🖾 🖄 🖆   9, @ @ @ 🗿 💆 🚍   🚍   9, 9, 9, 9, II								
	kap 🛛 🔍 Expression +									
N	o.	Time	Source	Destination	Protocol	Lengt Info	^			
	209	7 231.107_	172.16.1.2	172.16.1.126	LDAP	-220 searchResDone(2) noSuchObject (0000208D: NameErr: DSID-03100241, problem 2001 (NO_OBJECT), data 0, best mat	-			
	285:	329.849_	172.16.1.126	172.16.1.2	LDAP	99 bindRequest(1) "adadmin2@SBCSLAB.LOCAL" simple				
	2853	329.883_	172.16.1.2	172.16.1.126	LDAP	76 bindResponse(1) success				
	2854	329.883 <b>_</b>	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 result]				
	285	5 329.897_	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: Nicrosof_01:7e:01 (00:15:5d:01:7e:01), Dst: Cisco_44:57:7f (ec:bd:ld: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; LOAPMessage searchResDurty(2) "CN-adadmin2_CN=Users_DC=sbcslab_DC=local" [1 result] &gt; LOAPMessage searchResDone(2) success [1 result]</pre>									

## 如果不從全名欄位中取出空格會發生什麼?

如果嘗試使用*使用者登入名(本例中為adadmin*),您將看到登入失敗,因為輕量級目錄訪問協定 (LDAP)伺服器無法返回對象,因為*全名(本例中為ad admin1)有一個空格。*捕捉資料包時,您將能 夠看到這些詳細資訊,如下面的截圖所示。

## 結論

現在,您已成功完成並避免了通過RV34x路由器上的Active Directory進行遠端身份驗證的登入失敗。