Active Directory 및 RV34x 라우터를 사용하는 원 격 인증 및 로그인 지침

목표

이 문서에서는 Cisco RV34x Series 라우터에서 Windows AD(Active Directory)를 사용하여 원격 인 증을 구성하는 방법에 대해 설명합니다.또한 잠재적인 로그인 오류를 방지하기 위해 정보가 제공됩 니다.

소개

RV34x 라우터에서 서비스 인증 설정을 구성할 때 외부 인증 방법을 선택해야 합니다.

기본적으로 RV34x 시리즈 라우터의 외부 데이터베이스 우선순위는 RADIUS/LDAP/AD/Local입니 다.라우터에 RADIUS 서버를 추가하면 웹 로그인 서비스 및 기타 서비스에서 RADIUS 외부 데이터 베이스를 사용하여 사용자를 인증합니다.웹 로그인 서비스에만 외부 데이터베이스를 사용하도록 설정하고 다른 서비스에 대해 다른 데이터베이스를 구성하는 옵션은 없습니다.라우터에서 RADIUS를 생성하고 활성화하면 라우터는 웹 로그인, Site-to-Site VPN, EzVPN/타사 VPN, SSL VPN, PPTP/L2TP VPN 및 802.1x에 대한 외부 데이터베이스로 RADIUS 서비스를 사용합니다.

Windows를 사용하는 경우 Microsoft는 내부 AD 서비스를 제공합니다.AD는 사용자, 디바이스, 정책 을 포함하여 네트워크에 필요한 모든 필수 정보를 저장합니다.관리자는 AD를 단일 장소로 사용하 여 네트워크를 생성하고 관리합니다.상호 연결되고 복잡하며 서로 다른 네트워크 리소스와 통합된 방식으로 작업할 수 있습니다.

구성된 후에는 인증된 모든 사용자가 RV34x 라우터의 특정 서비스를 사용하도록 외부 AD 옵션 (Windows 서버 OS에 있음)을 사용하여 인증할 수 있습니다.인증된 사용자는 해당 인증 유형을 사 용하는 데 필요한 하드웨어 및 소프트웨어가 있는 한 제공된 기능을 사용할 수 있습니다.

적용 가능한 디바이스 | 소프트웨어 버전

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

목차

- <u>DN 값 식별</u>
- <u>Active Directory용 사용자 그룹 만들기</u>
- <u>RV34x 라우터에 Active Directory 세부 정보 추가</u>
- 전체 이름 필드에서 공간을 제거하지 않으면 어떻게 됩니까?

DN 값 식별

Windows 2016 서버*에서 Active Directory 사용자 및 컴퓨터* 관리 인터페이스에 액세스합니다.**사용 자** 컨테이너 폴더를 선택하고 마우스 오른쪽 버튼을 클릭한 다음 속성을 엽니다.나중에 RV34x 라 우터 *User Container Path* 필드에서 사용할 DistinguishedName 값*을* 기록합니다.

File Action Media Clipboard View Help		
🖴 💿 💿 🔕 💵 🕨 🔂 5 🖳		
Active Directory Users and Computers		

Active Directory용 사용자 그룹 만들기

1단계

RV34x 시리즈 라우터에 로그인합니다.System Configuration(**시스템 컨피그레이션) > User** Groups(사용자 그룹)로 이동합니다.



2단계

더하기 아이콘을 클릭합니다.



3단계

그룹 이름을 입력합니다.Apply를 **클릭합니다**.

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

이 예에서는 RemoteAdmin 사용자 그룹이 생성되었습니다.

새 사용자 그룹 옆의 확인란을 클릭합니다. 수정 아이콘을 클릭합니다.



Apply를 클릭합니다.



7단계

이제 새 사용자 그룹이 관리자 권한으로 표시됩니다.

			E	cisco R\	√345P-router4491EF				cisco (admir) English	• 🕜	0
⊗	Getting Started	U	ser	r Groups						A	oply	Car
•	Status and Statistics											
<u> </u>			User	Groups Table								
P	System Configuration		+	e 1								
	System			Group 🗢	Web Login/NETCONF/RESTCONF \$	S2S-VPN 🗢	EzVPN/3rd Party 🗢	SSL VPN 🗢	PPTP 🗢	L2TP 🗢	802.1x :	¢
	System Time			Group € RemoteAdmin	Web Login/NETCONF/RESTCONF \$	S2S-VPN 🗢	EzVPN/3rd Party \$	SSL VPN 🗢 Disabled	PPTP 🗢 Disabled	L2TP ♦ Disabled	802.1x	÷
	System Time Log			Group 🕈 RemoteAdmin admin	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	÷
	System Time Log Email			Group 🗣 RemoteAdmin admin anyconnect	Web Login/NETCONF/RESTCONF \$ Admin Admin Disabled	S2S-VPN \$	EzVPN/3rd Party \$ Disabled Disabled Disabled	SSL VPN \$ Disabled SSLVPNDef SSLVPNDef	PPTP \$ Disabled Enabled Disabled	L2TP \$ Disabled Enabled Disabled	802.1x = Disabled Enabled Disabled	¢
	System Time Log Email User Accounts			Group ¢ RemoteAdmin admin anyconnect guest	Web Login/NETCONF/RESTCONF ¢ Admin Admin Disabled Disabled	S2S-VPN ♦ 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	÷

RV34x 라우터에 Active Directory 세부 정보 추가

1단계

System **Configuration > User Accounts로 이동합니다.**AD 옵션을 선택하고 **수정 아이콘**을 클릭하여 AD 서버에 대한 세부 정보를 추가합니다.

		E	cisco	RV345P-route	er4491EF	l	cisco (admin)	English 🔻 ?	₿ 🕩						
\otimes	Getting Started	Use	er Accou	ints				Apply	Cancel						
•	Status and Statistics														
**	Administration	* Sho	Should have at least one account in the "admin" group												
• (System Configuration	Der													
	System 1	Rer	mote Authentication Service												
	Time	Rei	mote Authent	ication Service Tab	ble				^						
	Log	4	• 🕜 🖻												
	Email	C	Enable \$	Name 🗢	Primary Server 🗢	В	ackup Server \$								
	User Accounts 2		8 0	AD 3											
	User Groups	C		LDAP											
	IP Address Groups	C		RADIUS											
	SNMP														
	Discovery-Bonjour	* Plea	ase input remo	te authentication se	ervice configurations when it is enabled.										

2단계

AD *도메인 이름*, 기본 *서버*, *포트* 및 *사용자 컨테이너 경로* 세부 정보를 입력합니다.Apply를 **클릭합** 니다.

RV345P-router4491EF		cisco (RemoteAdmin)	English 🗸 ?	1 🕩				
User Accounts			Apply	Cancel				
Add/Edit New Domain								
Authentication Type Active Directory								
AD Domain Name sbcslab.local								
Primary Server 172.16.1.2	Port 389	0						
User Container Path cn=user,dc=sbcslab,dc=loc		J						

참고:Windows 서버에서 캡처된 *사용자 컨테이너 경로* 세부 정보를 이 기사<u>의 Identify the</u> <u>Distinguished Name Value</u> 섹션<u>에</u> 입력해야 합니다.

이 예에서 세부 정보는 *Cn=user,dc=sbcslab,dc=local입니다*.LDAP(Lightweight Directory Access Protocol) 서버 기본 수신 대기 포트는 389입니다.

3단계

AD에서 사용자 그룹이 구성되었고 라우터의 사용자 그룹 이름과 일치하는지 확인합니다.

	Hie Action Media Clipboard View Help	
1		
	Active Directory Users and Computers -	\times
	F File Action View Help	
	← ⇒ 2 📅 ¼ 📋 🗙 🗐 @ 🖦 🛛 🗊 🐍 🔌 🏗 🍸 🗵 🍇	
	Active Directory Users and Computers [sbcslabfores Name Type	
	Saved Queries	
	sbcstab.local	
	Builtin Security Group - Global	

4단계

*새 객체 - 사용자*에서 *이름*, *이니셜* 및 성을 입력하면 전체 *이름 필드가 자동으로 채워지며 성과 이 름 사이의 공백을 표시합니다.*

전체 이름 상자의 이름과 성 사이의 공백을 삭제해야 합니다. 그렇지 않으면 제대로 로그인하지 않 습니다.

이 그림에서는 삭제해야 하는 전체 이름의 공간을 보여 줍니다.

File Action Media Clipboard View Help		
🗄 🕘 💿 🔕 🖬 🕩 🔂 🍮 🗒	2	
Active Directory Users and Computers		
File Action View Help		
(++) 🖄 📷 🔏 🖬 🗶 🖼 🙆	8 🖬 🙎 📚 🗑 🍸 🚨 🗞	
Active Directory Users and Computers [sb Saved Queries Source Queries Domain Controllers Domain Controllers Domain Controllers Domain Controllers Domain Controllers Domain Controllers Managed Service Accounts Drogram Dat System System TPM Devices	Name RemoteAdmin RemoteAdmin Enterprise Admin Enterprise Admin Admin User2 Admin User3 AdminUser0 AdminUser1 Enterprise Iser I user logon name RemoteAdmin Enterprise Read-o RemoteAdmin R	Type Security Group - Global Security Group - Global r × e in: sbcslab.local/Users admin1 ad admin1 ad admin1 c @sbcslab.local v (gebcslab.local v)
	S sbcsadlabadmin1 S User 0 User 1	< Back Next > Cancel User

5단계

단계를 반복하여 다른 사용자를 생성합니다.다시 한 번, 자동으로 생성된 공백을 제거하여 *전체 이 름* 필드를 수정해야 합니다.Next(다음)를 클릭하여 비밀번호를 설정하고 사용자 생성을 완료합니다

이 그림에서는 전체 이름의 공간이 삭제되었음을 보여 줍니다.사용자를 추가하는 올바른 방법은 다 음과 같습니다.

File Action Media Clipboard View Help		
🗄 🕘 🖲 🕘 🖸 🖬 🕩 🍢 🌢 🕴	8	
Active Directory Users and Computers		
File Action View Help		
🗢 🔶 📶 🤾 🗙 🗟 🖬 🛛	1 🕇 📚 🏛 🖤 🚨 🗞	
Active Directory Users and Computers [sb Saved Queries Saved Queries Saved Queries Social Subtim Computers Domain Controllers Domain Controllers ForeignSecurityPrincipals Keys LostAndFound Managed Service Accounts	Name New Object - User RemoteAv Enterprise Enterprise Create in: sbcslab.local/Users Enterprise First nume: Admin Us Last name: Admin Us Full name: Admin Us Full name:	×
 Program Data System Users NTDS Quotas 	Administr AdminUst AdminUst AdminUst adadmin2 @sbcslab.local	
> TPM Devices	E Guest User logon name (pre-Windows 2000):	
	& L2TP User	
	Priv15 adr SBCS adm SBCS adm SbCs labadmin1 User User	incel

6단계

Users(사용자) 목록에는 새로 추가된 사용자 세부사항이 모두 표시됩니다.

File Action Media Clipboard View Help		
🗄 🔘 🔳 🞯 🤩 🖬 🕩 📳		
Active Directory Users and Computers		
File Action View Heln		
	m 🕅 🐮 🗽 🛍 🐨 🔎 🕼	
 Active Directory Users and Computers [sb Saved Queries Saved Queries Sultin Computers Domain Controllers ForeignSecurityPrincipals Keys LostAndFound Managed Service Accounts Program Data System Users NTDS Quotas TPM Devices 	Name Enterprise Admins Enterprise Key Admins Enterprise Read-only Domain Controllers Enterprise Read-only Domain Controllers Schema Admins Admin User2 Admin User3 Admin User4 Administrator AdminUser1 DefaultAccount Guest krbtgt L2TP User1 Priv15 admin SBCS admin	Type Security Group - Universal Security Group - Universal Security Group - Universal Security Group - Universal User User User User User User User User
	 sbcs labadmin1 sbcsadlabadmin1 User 0 User 1 User 2 User 3 User 4 User 5 User 5 User 6 User 7 User 8 User 9 ad admin1 	User User User User User User User User
< >	🍝 adadmin2	User

7단계

ad admin 1에 이름과 성 사이에 공백이 표시됩니다. 이 값이 수정되지 않으면 로그인이 실패합니다.이 오류는 데모용으로 남겨둔 것이므로 공간을 비워두지 마십시오!adadmin2 예제가 맞습니다.

보려면 ad admin *1* 사용자 이름을 마우스 오른쪽 버튼으로 클릭하고 **Properties** 옵션을 선택합니다 .그런 다음 **객체** 탭으로 이동하여 *객체* 세부사항*의 정식 이름을* 확인합니다.

ad admin1 Prop	perties			?	\times	Se Se	adadmin2 F	Properties				?	\times
Security Remote Dea	Environment sktop Services Profile	Sess C(Sessions Remote control COM+ Attribute Editor		ntrol ditor	U U	Security Remote	E Desktop S	nvironment ervices Profile	Sessions COM+		Remote control Attribute Editor	
General A Published Certif	ddress Account ficates Member Of	Profile Password	Telephones Replication	Orgar Dial-in	oization Object	UUU	General Published (Address Certificates	Account Member Of	Profile Passwor	Telephone d Replication	s Organ Dial-in	nization Object
sbeslab.local	ne of object: /Users/ad admin1					U U	Canonica sbcslab.lo	barne of of boal/Users/	adadmin2				
Object class:	User					U	Object cla	ess: U	ser				

또한 Properties(속성) 옵션 아래 *Member Of(구성원)* 탭으로 이동하여 해당 사용자 이름에 대한 Domain Users(*도메인 사용자*) 및 *RemoteAdmin* 세부 정보를 확인할 수 있습니다.



속성 편집기 탭으로 이동하여 해당 사용자 이름에 대한 DistinguishedName 값을 확인합니다.

ad admin1 Properties			?)	× Sa	dadmin2 P	roperties				?	Х
Security Er	nvironment	Sessions	Remote control	U	Security	Er	nvironment	Sess	ions F	emote control	
General Address	Account	Profile Teleph	ones Organizatio	on U	General	Address	Account	Profile	Telephones	Organizati	on
Published Certificates	Member Of	Password Replicat	ion Dial-in Obie	ect U	Published C	ertificates	Member Of	Passwor	d Replication	Dial-in Obi	ect
Remote Desktop S	ervices Profile	COM+	Attribute Editor	U	Remote	Desktop Se	ervices Profile	C	OM+ /	Attribute Editor	
Attributes:				- U	Attributes:						
ribute	Value		^	U	tribute		Value			^	
partmentNumber	<not set=""></not>			U	faultClass	Store	<not set=""></not>				
scription	<not set=""></not>			U	partment		<not set=""></not>				
sktopProfile	<not set=""></not>				partment	lumber	<not set=""></not>				
stinationIndicator	<not set=""></not>			U U	escription		<not set=""></not>				
:playName	ad admin1			, i	esktopProf	ile	<not set=""></not>				
:playNamePrintable	<not set=""></not>			U	estinationIr	ndicator	<not set=""></not>				
:tinguishedName	CN=ad admin	1,CN=Users,DC=sb	cslab,DC=local	U	splayName	e	adadmin2				
i i i	ind odb		_	U	splayName	Printable	<not set=""></not>			_	
ASignature	<not set=""></not>			U	stinguishe	dName	CN=adadmin	2,CN=Use	ers,DC=sbcslab	,DC=local	
CorePropagationD	0x0 = ()			U	VISION		KHOUSE(2			_	
namicLDAPServer	<not set=""></not>			U	ASignatu	re	<not set=""></not>				
ployeeID	<not set=""></not>				CoreProp	agationD	0x0 = ()				
ployeeNumber	<not set=""></not>			U U	namicLD.4	PServer	<not set=""></not>				
ployeeType	<not set=""></not>		~		nployeeID		<not set=""></not>			\checkmark	
<			>	U	<					>	
Edit			Filter	U	Edit					Filter	

8단계

사용자 로그온 이름으로 로그인합니다. 이 경우 adadmin2는 로그인이 성공했음을 나타냅니다.

9단계

다음 스크린샷과 같이 패킷 캡처에 대한 세부 정보를 볼 수 있습니다.

	🖸 Capturing from Ethernet — 🗆 🗙									
Fil	e Edit	View G	o Capture Ana	lyze Statistics	Telephony	Wireless Tools Help				
A	•	•		> ⇒ 🖻 🛉 🕹		Q. Q. Q. III				
	ldap					🛛 🔤 💌 Expression	+			
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_OBJECT), data 0, best mat.	-			
	2851	329.849_	172.16.1.126	172.16.1.2	LDAP	99 bindRequest(1) "adadmin2@SBCSLA8.LOCAL" simple				
	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 result]				
	2856	329.897_	172.16.1.126	172.16.1.2	LDAP	61 unbindRequest(3)				
							¥			
> > > > >	> Frame 2855: 206 bytes on wire (1648 bits), 206 bytes captured (1648 bits) on interface 0 > Ethernet II, Src: Microsof 01:7e:01 (00:15:5d:01:7e:01), Dst: Cisco_44:57:7f) > Internet Protocol Version 4, Src: 172.16.1.2, Dst: 172.16.1.126 > Internet Protocol, Protocol, Src Port: 389, Dst Port: 59096, Seq: 23, Ack: 135, Len: 152 > Lightweight Directory Access Protocol > Lightweight Directory Access Protocol									
~	Light	weight Dir	ectory Access A	rotocol						
	> LD#	₽Message	searchResDone(2	?) success [1 r	esuit]					

전체 이름 필드에서 공간을 제거하지 않으면 어떻게 됩니까?

*사용자 로그온 이름*을 사용하려고 하면 이 경우 adadmin은 *전체 이름*이 ad admin1에 공간이 있기 때문에 LDAP(Lightweight Directory Access Protocol) 서버가 개체를 반환할 수 없으므로 로그인 실 패*를* 보게 됩니다.다음 스크린샷과 같이 패킷을 캡처할 때 해당 세부 정보를 볼 수 있습니다.



이제 RV34x 라우터의 Active Directory를 통해 원격 인증을 위한 실패한 로그인을 성공적으로 완료 하고 방지했습니다.