Remote-Authentifizierung und Anmeldeanleitung unter Verwendung von Active Directory und RV34x-Routern

Ziel

In diesem Artikel wird erläutert, wie Sie die Remote-Authentifizierung mithilfe von Windows Active Directory (AD) auf Routern der Cisco Serie RV34x konfigurieren. Darüber hinaus werden Informationen bereitgestellt, um einen möglichen Anmeldefehler zu vermeiden.

Einführung

Wenn Sie die Einstellungen für die Dienstauthentifizierung auf dem RV34x-Router konfigurieren, müssen Sie eine externe Authentifizierungsmethode auswählen.

Die Priorität der externen Datenbank auf dem Router der Serie RV34x lautet standardmäßig RADIUS/LDAP/AD/Local. Wenn Sie den RADIUS-Server auf dem Router hinzufügen, authentifizieren der Weblogin-Dienst und andere Dienste den Benutzer mithilfe der externen RADIUS-Datenbank. Es gibt keine Option, eine externe Datenbank nur für den Weblogin-Dienst zu aktivieren und eine andere Datenbank für einen anderen Dienst zu konfigurieren. Sobald RADIUS erstellt und auf dem Router aktiviert ist, verwendet der Router den RADIUS-Service als externe Datenbank für die Webanmeldung, das Site-to-Site-VPN, das VPN von EzVPN/Drittanbietern, das SSL VPN, das PPTP/L2TP VPN und 802.1x.

Wenn Sie Windows verwenden, stellt Microsoft einen internen AD-Dienst bereit. AD speichert alle wichtigen Informationen für das Netzwerk, einschließlich Benutzer, Geräte und Richtlinien. Administratoren verwenden AD als eine zentrale Stelle für die Erstellung und Verwaltung des Netzwerks. Sie vereinfacht die einheitliche Verwendung von miteinander verbundenen, komplexen und unterschiedlichen Netzwerkressourcen.

Nach der Konfiguration kann sich jede autorisierte Person mithilfe der externen AD-Option (im Windows Server-Betriebssystem vorhanden) authentifizieren, um einen bestimmten Dienst auf dem RV34x-Router zu verwenden. Autorisierte Benutzer können die bereitgestellten Funktionen verwenden, sofern sie über die erforderliche Hardware und Software für die Verwendung dieser Authentifizierungstypen verfügen.

Anwendbare Geräte | Softwareversion

- RV340 | 1.0.03.16
- RV340 W | 1.0.03.16
- RV345 | 1.0.03.16
- RV345P | 1.0.03.16

Inhaltsverzeichnis

- Identifizieren des Wertes für den Distinguished Name
- Erstellen einer Benutzergruppe für Active Directory
- Hinzufügen von Active Directory-Details zum RV34x-Router
- Was passiert, wenn Sie den Leerzeichen nicht aus dem Feld "Vollständiger Name" entfernen?

Identifizieren des Wertes für den Distinguished Name

Zugriff auf die Verwaltungsschnittstelle *Active Directory-Benutzer und -Computer* auf dem Windows 2016-Server. Wählen Sie den Ordner **Benutzer**-Container aus, klicken Sie mit der rechten Maustaste, und öffnen Sie **Eigenschaften**. Beachten Sie den Wert *DistinguishedName*, der später im *Feld* RV34x-Router *User Container Path* verwendet wird.



Erstellen einer Benutzergruppe für Active Directory

Schritt 1

Melden Sie sich beim Router der Serie RV34x an. Navigieren Sie zu **Systemkonfiguration > Benutzergruppen**.



Schritt 2

Klicken Sie auf das Pluszeichen.



Schritt 3

Geben Sie einen Gruppennamen ein. Klicken Sie auf Übernehmen.

RV345P-RV345P	English 🔹 😮 🚺 🕩
User Groups	2 Apply Cancel
Overview Group Name: RemoteAdmin 1	

In diesem Beispiel wurde eine RemoteAdmin-Benutzergruppe erstellt.

Schritt 4

Klicken Sie auf das Kontrollkästchen neben der neuen Benutzergruppe. Klicken Sie auf das **Bearbeitungssymbol**.



Schritt 5

Blättern Sie auf der Seite nach unten zu Dienste. Klicken Sie auf das Optionsfeld Administrator.

Services

Schritt 6

Klicken Sie auf Übernehmen.



Schritt 7

Die neue Benutzergruppe wird nun mit Administratorrechten angezeigt.

	E	cisco RV	V345P-router4491EF				cisco (admin	I) English	• 🕜 (
Getting Started	Use	er Groups							Apply
Status and Statistics									
System Configuration	Us	er Groups Table							
System		▪ 📝 前 〕 Group ≑	Web Login/NETCONF/RESTCONF \$	S2S-VPN 🗢	EzVPN/3rd Party \$	SSL VPN 🗢	PPTP 🗢	L2TP 🗢	802.1x ≑
Time	C	RemoteAdmin	Admin	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
Loa) admin	Admin	Disabled	Disabled	SSLVPNDef	Enabled	Enabled	Enabled
Email) anyconnect	Disabled	Disabled	Disabled	SSLVPNDef	Disabled	Disabled	Disabled

Hinzufügen von Active Directory-Details zum RV34x-Router

Schritt 1

Navigieren Sie zu **Systemkonfiguration > Benutzerkonten.** Wählen Sie die *AD*-Option aus, und klicken Sie auf das **Bearbeitungssymbol**, um die Details für den AD-Server hinzuzufügen.

		📑 ांग्व	RV345P-router	4491EF	💾 cisco (admin)	English 🔹 ?	() ()		
⊗	Getting Started	User Acco	ounts			Apply	Cancel		
•	Status and Statistics								
**	Administration	* Should have at	least one account in the	e "admin" group					
•	System Configuration								
	System 1	Remote A	uthentication						
	Time	Remote Auth	entication Service Tabl	e			^		
	Log	4+7							
	Email	Enable 4	Name ♦	Primary Server 🗢	Backup Server 🗢				
(User Accounts 2		AD 3						
	User Groups		LDAP						
	IP Address Groups		RADIUS						
	SNMP								
	Discovery-Bonjour	* Please input re	mote authentication ser	vice configurations when it is enabled.					

Schritt 2

Geben Sie die Details *AD-Domänenname*, *Primärserver*, *Port* und *Benutzercontainerpfad ein*. Klicken Sie auf **Übernehmen**.



Hinweis: Sie müssen die vom Windows-Server erfassten *User Container Path-*Details im Abschnitt Identify the Distinguished Name Value in diesem Artikel eingeben.

In diesem Beispiel sind die Details *Cn=user,dc=sbcslab,dc=local*. Der Standardüberwachungsport des LDAP-Servers (Lightweight Directory Access Protocol) ist 389.

Schritt 3

Überprüfen Sie im AD, ob die *Benutzergruppe* konfiguriert ist und mit dem *Benutzergruppennamen* des Routers übereinstimmt.

File Action Media Clipboard View Help		
🗄 🕲 💿 🕲 💵 🕨 🍢 🌣 🕎		
Active Directory Users and Computers F File Action View Help		– o x
🗢 🔿 🙋 📷 🖌 📋 🗙 🖼 🐼 🖬	🕺 🐮 🐨 🍞 🔟 🐍	
 Active Directory Users and Computers [sbcslabfores Saved Queries Solution Builtin Computers Domain Controllers ForeignSecurityPrincipals Keys LostAndFound Managed Service Accounts Program Data System Users NTDS Quotas TPM Devices 	Name Second Second Sec	Type Security Group - Universal Security Group - Global User Security Group - Global User User Security Group - Global User Security Group - Global Security Group - Global User User User
	Schema Admins	Security Group - Universal

Schritt 4

Unter Neues Objekt - Benutzer geben Sie den Vornamen, die Initialen und den Nachnamen ein, das Feld Vollständiger Name wird automatisch ausgefüllt, sodass ein Leerzeichen zwischen dem Vor- und Nachnamen angezeigt wird.

Der Abstand zwischen dem Vor- und dem Nachnamen im Feld Vollständiger Name muss gelöscht

werden, oder er meldet sich nicht richtig an.

Dieses Bild zeigt das Leerzeichen im vollen Namen, das gelöscht werden muss:



Schritt 5

Wiederholen Sie die Schritte, um einen anderen Benutzer zu erstellen. Sie müssen das Feld *Vollständiger Name* erneut ändern, indem Sie automatisch erstellte Leerzeichen entfernen. Klicken Sie auf **Weiter**, um das Kennwort einzurichten und die Erstellung des Benutzers abzuschließen.

Dieses Bild zeigt, dass das Leerzeichen im vollen Namen gelöscht wurde. So können Sie den Benutzer richtig hinzufügen:

File Action Media Clipboard View Help		
🗄 🕘 🖲 🥥 🖸 💷 🕞 😓 🗏	2	
Active Directory Users and Computers		
File Action View Help		
4 4 🔊 📷 X 🗙 🖬 🔒 🛛 🕫	n 🙁 🗽 fan 🐨 🗾 🗽	
Active Directory Users and Computers [sb Active Directory Users and Computers [sb Saved Queries Builtin Computers Domain Controllers E Domain Controllers E ForeignSecurityPrincipals E Keys E LostAndFound Program Data System Users MTDS Quotas TPM Devices	Name New Object - User RemoteA RemoteA Enterprise Create in: sbcslab.local/Users Enterprise First nume: Admin Us Last name: Admin Us Last name: Admin Us Admin2 AdminUs User logon name: AdminUs User logon name: AdminUs User logon name: AdminUs SBCSLAB\ BEDESLAB\ adadmin2 SBCS adm Cleack SBCS admin1 User Sbcsadlabadmin1 User User 0 User	At:
	🕹 User 1 User	
	🔏 User 2 User	

Schritt 6

Die Liste Benutzer zeigt beide neu hinzugefügten Benutzerdetails an.



Schritt 7

Sie werden feststellen, dass *admin1* ein Leerzeichen zwischen dem Vor- und Nachnamen anzeigt. Wenn dieser nicht behoben ist, schlägt die Anmeldung fehl. Dieser Fehler wird zu Demonstrationszwecken in gelassen, lassen Sie den Platz nicht dort! Das Beispiel *admin2* ist korrekt.

Klicken Sie zum Anzeigen mit der rechten Maustaste auf den Benutzernamen Admin 1 und wählen Sie die Option **Eigenschaften**. Navigieren Sie dann zur Registerkarte **Objekt**, um den *kanonischen Namen der Object*-Details anzuzeigen.

ad admin1 Prop	erties		? ×	S	adadmin2 Prop	perties		? ×
Security Remote Des	Environment ktop Services Profile	Sessions COM+	Remote control Attribute Editor	UU	Security Remote De	Environment sktop Services Profile	Sessions COM+	Remote control Attribute Editor
General Ac Published Certifi Canonical nam sbcslab.local/	ddress Account icates Member Of ne of object: Users/ad admin1	Profile Telep Password Replic	hones Organization ation Dial-in Object	U U U U	General A Published Certi Canonical par sbcslab.local	ddress Account ficates Member Of me of object: /Users/adadmin2	Profile Telep Password Replic	hones Organization ation Dial-in Object
Object class:	User			U	Object class:	User		

Sie können auch die *Domänenbenutzer* und die *RemoteAdmin-*Details für diese Benutzernamen überprüfen, indem Sie unter der Option Eigenschaften zur Registerkarte *Member Of navigieren*.



Navigieren Sie zur Registerkarte *Attribute-Editor*, um die *DistinguishedName*-Werte für diese Benutzernamen zu überprüfen.

d admin1 Pro	operties					?	\times	S	adadmin2 P	ropert	ties					?	>
Security	Er	nvironment	Sess	ions	Ren	note contr	rol	U	Security		Er	vironment	Ses	sions	Re	mote cor	ntrol
General /	Address	Account	Profile	Teleph	nones	Organiza	ation	U	General	Addr	ess	Account	Profile	Teleph	ones	Organ	izatio
Published Cer	tificates	Member Of	Passwor	d Replica	ation D	ial-in O	lbiect	U	Published 0	Certifica	ites	Member Of	Passwo	d Replica	tion	Dial-in	Obie
Remote D	esktop Se	ervices Profile	C	OM+	Attr	ribute Edit	tor	U	Remote	Deskt	op Se	ervices Profile	C	OM+	A	ttribute Eo	ditor
Attributes:								U	Attributes:								
ribute:		Value				^	•	U	tribute			Value					^
partmentNur	mber	<not set=""></not>						U	aultClass	Store		<not set=""></not>					
scription		<not set=""></not>						U	partment			<not set=""></not>					
sktopProfile		<not set=""></not>						-	partment	Numbe	ſ	<not set=""></not>					
stinationIndi	cator	<not set=""></not>						ŭ	escription			<not set=""></not>					
:playName		ad admin1							esktopProl	file		<not set=""></not>					
:playNamePr	rintable	<not set=""></not>				_		U	estination	ndicato	r	<not set=""></not>					
:tinguishedN	ame	CN=ad admir	n1,CN=Use	ers,DC=st	boslab,D1	C=local		U	splayNam	е		adadmin2					
		that acts				-		U	splayNam	ePrinta	ble	<not set=""></not>					
ASignature		<not set=""></not>						U	stinguishe	dName	;	CN=adadmir	n2,CN=Us	ers,DC=sb	cslab,[)C=local	
CorePropag	ationD	0x0 = ()						U	VISION			CHOUSE(2					•
namicLDAPS	Server	<not set=""></not>						U	SASignatu	re		<not set=""></not>					
1ployeeID		<not set=""></not>						U	CoreProp	agation	nD	0x0 = ()					
nployeeNumb	ber	<not set=""></not>							namicLD/	APServ	/er	<not set=""></not>					
пріоуееТ уре		<not set=""></not>	_			~	1	Ŭ	nployeeID			<not set=""></not>					~
<						>			<							>	
Edit						Filter		U	Edit							Filter	

Schritt 8

Melden Sie sich mit dem *Benutzernamen für die Anmeldung an*, in diesem Fall *admin2*, wird angezeigt, dass die Anmeldung erfolgreich war.

Schritt 9

Die Details zur Paketerfassung werden im folgenden Screenshot dargestellt.

🗹 Capturing from Ethernet 🧧 🗖										
Fil	e Edit	View G	o Capture Ana	lyze Statistics	Telephony	Wireless Tools Help				
Â		•	× • • •	÷ → ≌ 🚹 🌡		Q. Q. Q. II				
	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 m	at_		
	2851	329.849_	172.16.1.126	172.16.1.2	LDAP	99 bindRequest(1) "adadmin2@SBCSLAB.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	sult]			
	2856	329.897 <u>-</u>	172.16.1.126	172.16.1.2	LDAP	61 unbindRequest(3)				
	-			/				~		
>	Frame Etherr Interr	2855: 206 net II, Sr net Protoc	bytes on wire c: Microsof_01 ol Version 4. :	(1648 bits), 2 :7e:01 (00:15:5 Src: 172.16.1.2	206 bytes 5d:01:7e: 2. Dst: 1	captured (1648 bits) on intertace 0 01), Dst: Cisco_44:57:7f (ec:bd:1d:44:57:7f) 72.16.1.126				
>	Transm	nission Co	ntrol Protocol	, Src Port: 389	9, Dst Pc	rt: 59096, Seq: 23, Ack: 135, Len: 152				
Ľ	Light: ≻ LD4	veight Dir PMessage	ectory Access I searchResEntry	Protocol (2) "CN=adadmir	12,CN=Use	rs,DC=sbcslab,DC=local" [1 result]				
Y	Light	eight Dir	ectory Access I	Protocol	141					
	≠ LD#	+nessage	sear chkespone(2	2) success [1 r	esuitj					

Was passiert, wenn Sie den Leerzeichen nicht aus dem Feld "Vollständiger Name" entfernen?

Wenn Sie den *Benutzernamen* verwenden, in diesem Fall *admin*, wird die Anmeldung fehlschlagen, da der LDAP-Server (Lightweight Directory Access Protocol) das Objekt nicht zurückgeben kann, da *Vollname* in diesem Fall *ad admin1* einen Leerzeichen hat. Sie können diese Details beim Erfassen der Pakete sehen, wie im folgenden Screenshot gezeigt.

Schlussfolgerung

Sie haben jetzt eine fehlgeschlagene Anmeldung für die Remote-Authentifizierung über Active Directory auf dem RV34x-Router erfolgreich abgeschlossen und vermieden.