# Active DirectoryおよびRV34xルータを使用した リモート認証およびログインガイダンス

## 目的

この記事では、Cisco RV34xシリーズルータでWindows Active Directory(AD)を使用してリモート 認証を設定する方法について説明します。また、潜在的なログインエラーを回避するための情報 も提供されます。

### 概要

RV34xルータでサービス認証設定を設定する場合は、外部認証方式を選択する必要があります。

デフォルトでは、RV34xシリーズルータの外部データベースプライオリティは RADIUS/LDAP/AD/Localです。ルータにRADIUSサーバを追加すると、Webログインサービスや その他のサービスは、RADIUS外部データベースを使用してユーザを認証します。Webログイン サービス専用の外部データベースを有効にし、別のサービス用に別のデータベースを設定するオ プションはありません。ルータでRADIUSが作成され、有効になると、ルータはRADIUSサービス をWebログイン、サイト間VPN、EzVPN/3rd Party VPN、SSL VPN、PPTP/L2TP VPN、および 802.1xの外部データベースとして使用します。

Windowsを使用している場合、Microsoftは内部ADサービスを提供します。ADには、ユーザ、デ バイス、ポリシーなど、ネットワークに不可欠な情報がすべて保存されます。管理者は、ネット ワークを作成および管理するための単一の場所としてADを使用します。相互接続された複雑な異 なるネットワークリソースを一元的に扱いやすくします。

設定が完了すると、承認されたユーザは外部ADオプション(Windows Server OSに存在)を使用 して認証を行い、RV34xルータ上の特定のサービスを使用できます。権限のあるユーザは、その タイプの認証を使用するために必要なハードウェアとソフトウェアがある限り、提供された機能 を使用できます。

### 該当するデバイス |ソフトウェアバージョン

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

## 目次

- ・<u>識別名の値の特定</u>
- <u>Active Directoryのユーザグループの作成</u>
- <u>RV34xルータでのActive Directoryの詳細の追加</u>
- 完全な名前フィールドからスペースを取らないとどうなりますか。

## 識別名の値の特定

Windows 2016サーバのActive Directoryユーザーとコンピューターの管理インターフェイスにアク セスします。Usersコンテナフォ**ルダを選**択し、マウスを右クリックして[プロパティ]を**開きま**す

#### 。後でRV34xルータの*User Container Path*フィールドで使用するDistinguishedNameの値を書*き 留め*ま*す*。



# Active Directoryのユーザグループの作成

## 手順 1

RV34xシリーズルータにログインします。[System Configuration] > [User Groups]に移動します。



### 手順 2

[+]アイコンを**クリックします**。





#### グループ名を入力します。[Apply] をクリックします。

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

この例では、RemoteAdminユーザーグループが作成されています。

### 手順 4

新しいユーザグループの横にあるチェックボックスをクリックします。編集アイコンを**クリック** します。





## ステップ7

#### 新しいユーザグループが管理者権限で表示されます。

		cisco	/345P-router4491EF				cisco (admin	) English •	00
🖏 Getting S	itarted	lser Groups						Ap	ply Ca
Status an	d Statistics								
Administr	ration	User Groups Table							
System C	Configuration	▲ 🖓 🚔							
System									
		□ Group <del>\$</del>	Web Login/NETCONF/RESTCONF \$	S2S-VPN 🗢	EzVPN/3rd Party 🗢	SSL VPN 🗢	PPTP 🗢	L2TP 🗢	802.1x 🗢
Time		□ Group ≑	Web Login/NETCONF/RESTCONF 🗢	S2S-VPN 🗢	EzVPN/3rd Party \$	SSL VPN \$	PPTP 🗢	L2TP 🖨	802.1x ≎ Disabled
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
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 \$	EzVPN/3rd Party \$ Disabled Disabled Disabled	SSL VPN \$ Disabled SSLVPNDef SSLVPNDef	PPTP ♦ Disabled Enabled Disabled	L2TP \$ Disabled Enabled Disabled	802.1x ¢ Disabled Enabled Disabled
Time Log Email User Acc	ounts	<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	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

## RV34xルータでのActive Directoryの詳細の追加

### 手順 1

[システム構成] > [**ユーザーアカウント]に移動します。**ADオプション*を選択*し、編集アイコン**を** クリックして、ADサーバの詳細を追加します。

		E	cisco	RV345P-rout	iter4491EF	E	cisco (admin)	English 🔹 ?	<b>()</b> ()
$\otimes$	Getting Started	Use	r Accou	nts				Apply	Cancel
•	Status and Statistics								
**	Administration	* Shou	ıld have at lea	st one account in	the "admin" group				
<b>\$</b> (	System Configuration System	Ren	note Aut	henticatior	n Service				
	Time	Ren	note Authent	cation Service Ta	Fable				^
	Log	4+							
	Email		Enable \$	Name 🖨	Primary Server 🗢	В	ackup Server 🗢		
(	User Accounts 2			AD 3					
	User Groups			LDAP					
	IP Address Groups	0	0	RADIUS					
	SNMP								
	Discovery-Bonjour	* Pleas	se input remo	te authentication s	service configurations when it is enabled.				

## 手順 2

[AD Domain Name]、[Primary Server]、[Port]、および[User Container Path]の詳細を入力します。 。[Apply] をクリックします。

RV345P-router4491EF	cisco (RemoteAdmin) English 🗸 ? 🚺 🕩
User Accounts	Apply Cancel
Add/Edit New Domain	
Name AD	
AD Domain Name	
Primary Server 172.16.1.2 Port 389	V
User Container Path cn=user,dc=sbcslab,dc=loc	

**注**:この記事の「識別名の識別*」セクション*で、Windowsサーバから取得したユーザコンテナ<u>パ</u> <u>スの詳細を入力する</u>必要があります。

この例では、詳細は*Cn=user,dc=sbcslab,dc=localです*。Lightweight Directory Access Protocol(LDAP)サーバのデフォルトのリスニングポートは389です。

### 手順 3

ADで、ユーザグループが設定さ*れ、ルータの*ユーザグループ名と一致していることを*確認し*ま*す* 

File Action Media Clipboard View Help		
Active Directory Users and Computers File Action View Help File Action View Help Active Directory Users and Computers [sbcslabfores	Name	— — ×
<ul> <li>Solution Gutters</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>	Enterprise Read-only Domain Controllers     Group Policy Creator Owners     Guest     Key Admins     Key Admins     L2TP User1     L2TPVPN     PPTP User1     PPTPVPN     PPTPVPN     Priv15 admin     Priv15Admins     Protected Users     RAS and IAS Servers     Read-only Domain Controllers	Security Group - Universal Security Group - Global User Security Group - Global User User Security Group - Global User Security Group - Global Security Group - Global Security Group - Global Security Group - Global
	SBCS admin sbcs labadmin1 schema Admins	Security Group - Global User User User Security Group - Universal

#### 手順 4

[New Object - User]で、[*First name*]、[*Initials*]、[*Last name*]を入力します。[*Full name*]フィールド は自動的に入力され、姓と名の間のスペースが表示されます。

[フルネーム]ボックスの名と姓の間のスペース*を削除する*必要があります。削除しないと、正しく ログインできません。 次の図は、削除する必要があるフルネームのスペースを示しています。



#### 手順5

手順を繰り返して、別のユーザを作成します。ここでも、自動的に作成されたスペースを削*除して[*フルネーム]フィールドを変更する必要があります。[次へ]をクリ**ック**して、パスワードを設定し、ユーザの作成を終了します。

次の図は、フルネームのスペースが削除されたことを示しています。ユーザを追加する正しい方 法は次のとおりです。



#### [Users]リストには、新しく追加されたユーザの詳細が両方とも表示されます。



## ステップ7

ad admin1は姓と名の間にスペースを表示します。このスペースが修正されていない場合、ログインは失敗します。このエラーはデモ用に残されています。スペースを残さないでください。 adadmin2*の例*が正しいです。

表示するには、ad admin 1ユーザ名を右クリック*し、[プロパティ*]オプションを**選択**します。次に、[オブジェクト]タブに移動し、オブジェクトの正規名の詳細を確認します。

ad admin1 Properties ? ×					adadmin2 Prop	perties			? ×
Security Environment Sessions Remote Desktop Services Profile COM+			Remote control Attribute Editor		Security Remote De	Environme sktop Services F	nt Ses rofile (	sions F	Remote control Attribute Editor
General A/ Published Certif Canonical nan sbcslab.local/ Object class:	ddress Accoun icates Member 0 ne of object: 'Users/ad admin1 User	Profile Telep f Password Replic	hones Organization ation Dial-in Object	U U U U U U	General A Published Certi Canonical par sbcslab.local Object class:	ddress Acco ficates Membr me of object /Users/adadmin User	unt Profile er Of Passwo 2	T elephones rd Replication	Organization Dial-in Object

また、[Properties]オプションの[*Member Of*]タブに移動することにより、これらのユーザ名の[ *Domain Users*]および[*RemoteAdmin*]の詳細を確認で**きま**す。



### [Attribute Editor]タブに移動し、それらのユーザ名のDistinguishedName値を確認します。

id admin1 Properties			? ×	× adadmin2 Prop	perties		? X
Security Er	nvironment	Sessions	Remote control	U Security	Environment	Sessions	Remote control
General Address	Account	Profile Telep	hones Organization	n U General A	Address Account	Profile Telephone	s Organization
Published Certificates	Member Of	Password Replic	ation Dial-in Object	ct U Published Certi	ificates Member Of	Password Replication	Dial-in Obiec
Remote Desktop S	ervices Profile	COM+	Attribute Editor	U Remote De	sktop Services Profile	COM+	Attribute Editor
Attributes:				U Attributes:			
ribute	Value		^	U tribute	Value		^
partmentNumber	<not set=""></not>			U efaultClassSto	ore <not set=""></not>		
scription	<not set=""></not>			partment	<not set=""></not>		
sktopProfile	<not set=""></not>			partmentNur	nber <not set=""></not>		
stinationIndicator	<not set=""></not>			escription	<not set=""></not>		
:playName	ad admin1			esktopProfile	<not set=""></not>		
playNamePrintable	<not set=""></not>			UestinationIndic	cator <not set=""></not>		
tinguishedName:	CN=ad admin	n1,CN=Users,DC=:	sbcslab,DC=local	U splayName	adadmin2		
				U splavNamePri	intable <not set=""></not>		
ASignature	<not set=""></not>			U stinguishedNa	ame CN=adadmin	2,CN=Users,DC=sbcsla	ab,DC=local
CorePropagationD	$0 \times 0 = ()$			U	CHOC SEC/		_
namicLDAPServer	<not set=""></not>			) BASignature	<not set=""></not>		
ployeeID	<not set=""></not>			CorePropage	ationD 0x0 = ( )		
ployeeNumber	<not set=""></not>			namicLDAPS	Server <not set=""></not>		
ployeeType	<not set=""></not>		~		<not set=""></not>		~
<			>	<			>
Edit			Filter	U Edit			Filter

### 手順 8

*User logon name*(この場合は*adadmin2*)を使用してログインすると、ログインが正常に行われた ことが分かります。

### 手順 9

次のスクリーンショットに示すように、パケットキャプチャの詳細を確認できます。

	Capturing from Ethemet -											
Fil	e Edit	Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help										
1				> -> 🕾 🗿 🕹		Q. Q. Q. II						
	Idap					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	t					
	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 <u>-</u>	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 <b>_</b>	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: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; LDAPMessage searchResEntry(2) "CN=adadmin2,CN=Users,DC=bcslab,DC=local" [1 result] &gt; LOAPMessage searchResDone(2) success [1 result]</pre>											

## 完全な名前フィールドからスペースを取らないとどうなりますか

0

ユーザーログオン名を使用しようとすると、adadminが表示され、Lightweight Directory Access Protocol(LDAP)サーバーはオブジェクトを返すことができません。この場合はad admin1にスペ ースが入っています。次のスクリーンショットに示すように、パケットをキャプチャすると、そ の詳細が表示されます。



これで正常に完了し、RV34xルータのActive Directoryを介したリモート認証のログイン失敗を回 避できました。