# Guida all'autenticazione e al login remoti tramite router Active Directory e RV34x

## Obiettivo

In questo articolo viene spiegato come configurare l'autenticazione remota con Windows Active Directory (AD) sui router Cisco serie RV34x. Verranno inoltre fornite informazioni per evitare possibili errori di accesso.

## Introduzione

Quando si configurano le impostazioni di autenticazione del servizio sul router RV34x, è necessario selezionare un metodo di autenticazione esterno.

Per impostazione predefinita, la priorità del database esterno sul router della serie RV34x è RADIUS/LDAP/AD/Local. Se si aggiunge il server RADIUS al router, il servizio Accesso Web e altri servizi utilizzeranno il database esterno RADIUS per autenticare l'utente. Non è disponibile alcuna opzione per abilitare un database esterno solo per il servizio Accesso Web e configurare un altro database per un altro servizio. Dopo aver creato e abilitato RADIUS sul router, questo utilizzerà il servizio RADIUS come database esterno per login Web, VPN da sito a sito, VPN EzVPN/di terze parti, VPN SSL, PPTP/L2TP VPN e 802.1x.

Se si utilizza Windows, Microsoft offre un servizio AD interno. AD archivia tutte le informazioni essenziali per la rete, inclusi utenti, dispositivi e criteri. Gli amministratori utilizzano Active Directory come posizione singola per creare e gestire la rete. Semplifica il lavoro con risorse di rete interconnesse, complesse e diverse in modo unificato.

Una volta configurata, chiunque sia autorizzato può eseguire l'autenticazione utilizzando l'opzione AD esterna (presente nel sistema operativo Windows server) per utilizzare qualsiasi servizio specifico sul router RV34x. Gli utenti autorizzati possono utilizzare le funzionalità fornite, a condizione che dispongano dell'hardware e del software necessari per utilizzare quel tipo di autenticazione.

## Dispositivi interessati | Versione software

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

## Sommario

- Identificare il valore del nome distinto
- Crea un gruppo di utenti per Active Directory
- <u>Aggiunta di dettagli di Active Directory sul router RV34x</u>
- <u>Cosa succede se non si estrae lo spazio dal campo del nome completo?</u>

## Identificare il valore del nome distinto

Accedere all'interfaccia di gestione *Utenti e computer di Active Directory* nel server Windows 2016. Selezionare la cartella contenitore **Users**, fare clic con il pulsante destro del mouse e aprire **Proprietà**. Prendere nota del valore *DistinguishedName* che verrà utilizzato in seguito nel campo *Percorso contenitore utente* router RV34x.



## Crea un gruppo di utenti per Active Directory

## Passaggio 1

Accedere al router della serie RV34x. Passare a Configurazione di sistema > Gruppi di utenti.



Passaggio 2

Fare clic sull'icona più.



#### Passaggio 3

Immettere il nome di un gruppo. Fare clic su Apply (Applica).



In questo esempio è stato creato un gruppo di utenti RemoteAdmin.

## Passaggio 4

Fare clic sulla casella di controllo accanto al nuovo gruppo di utenti. Fare clic sull'icona Modifica.



#### Passaggio 5

Scorrere la pagina fino a Servizi. Fare clic sul pulsante di opzione Amministratore.



## Passaggio 6

Fare clic su Apply (Applica).



## Passaggio 7

Verrà visualizzato il nuovo gruppo di utenti con privilegi di amministratore.

		3	cisco R\	/345P-router4491EF				cisco (admin	) English	• 🕜 🤅
<b>&gt;</b>	Getting Started	Use	r Groups						A	pply
	Administration		0							
	System Configuration	Use	r Groups Table							
	System		Group 🗢	Web Login/NETCONF/RESTCONF \$	S2S-VPN \$	EzVPN/3rd Party 🗢	SSL VPN \$	PPTP \$	L2TP 🖨	802.1x 🖨
	lime		RemoteAdmin	Admin	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
	lime Log		RemoteAdmin	Admin Admin	Disabled Disabled	Disabled Disabled	Disabled SSLVPNDef	Disabled Enabled	Disabled Enabled	Disabled Enabled
	Time Log Email		RemoteAdmin admin anyconnect	Admin Admin Disabled	Disabled Disabled Disabled	Disabled Disabled Disabled	Disabled SSLVPNDef SSLVPNDef	Disabled Enabled Disabled	Disabled Enabled Disabled	Disabled Enabled Disabled

## Aggiunta di dettagli di Active Directory sul router RV34x

## Passaggio 1

Passare a **Configurazione di sistema > Account utente.** Selezionare l'opzione *AD* e fare clic sull' **icona Modifica** per aggiungere i dettagli per il server AD.

		€	ılıılı cısco	RV345P-route	er4491EF			cisco (admin)	English 🔹 ?	<b>6</b> 🕩
$\otimes$	Getting Started	User	Accou	nts					Apply	Cancel
•	Status and Statistics	0001	, 100004						coppy	
쌸	Administration	* Should	have at leas	st one account in th	he "admin" group					
<b>\$</b> (	System Configuration System	Remo	ote Aut	hentication	Service					
	Time	Remo	te Authenti	cation Service Tab	ble					^
	Log	4+	<b>B</b>							
	Email		Enable \$	Name 🗢	Primary Server 🗢		Backup	Server 🗢		
(	User Accounts 2		0	AD 3						
	User Groups			LDAP						
	IP Address Groups	0 0		RADIUS						
	SNMP									
	Discovery-Bonjour	* Please	input remot	e authentication se	ervice configurations when it is enal	bled.				

## Passaggio 2

Immettere i dettagli *Nome dominio Active Directory, Server primario, Porta* e *Percorso contenitore utente.* Fare clic su **Apply** (Applica).



**Nota:** È necessario immettere i dettagli relativi al *percorso del contenitore utente* acquisiti dal server Windows nella sezione <u>Identificare il valore del nome distinto</u> di questo articolo.

In questo esempio, i dettagli sono *Cn=user,dc=sbcslab,dc=local*. La porta di ascolto predefinita del server Lightweight Directory Access Protocol (LDAP) è 389.

#### Passaggio 3

In Active Directory verificare che il *gruppo di utenti* sia configurato e che corrisponda al nome del *gruppo di utenti* del router.

File Action Media Clipboard View Help		
=   💿 💿 🔕   💵 🕨   💺 🗅   🕎		
Active Directory Users and Computers File Action View Help		– 🗆 X
🗢 🔿 🔁 📆 🦌 🗎 🗙 🖼 🧟 🕞 🛛 🖬	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>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 Renterprise Read-only Domain Controllers Group Policy Creator Owners Guest Key Admins Krbtgt L2TP User1 L2TP VPN PTP User1 PTPVPN PTPVPN Priv15 admin Priv15Admins RAS and IAS Servers RAS and IAS Servers Read-only Domain Controllers SBCS admin Sbcs labadmin1 Sbcs albadmin1	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

#### Passaggio 4

In Nuovo oggetto - Utente, compilare *Nome*, *Iniziali* e *Cognome*, il *campo Nome completo* verrà compilato automaticamente, mostrando uno spazio tra il nome e il cognome.

Ènecessario eliminare lo spazio tra il nome e il cognome nella casella *Nome completo* per evitare che il login venga eseguito correttamente.

Nell'immagine è illustrato lo spazio da eliminare nel nome completo:



#### Passaggio 5

Ripetere i passaggi per creare un altro utente. È necessario modificare nuovamente il campo *Nome completo* rimuovendo gli spazi creati automaticamente. Fare clic su **Avanti** per impostare la password e completare la creazione dell'utente.

Nell'immagine è illustrato che lo spazio nel nome completo è stato eliminato. Questo è il modo corretto per aggiungere l'utente:



## Passaggio 6

Nell'elenco Utenti verranno visualizzati entrambi i dettagli appena aggiunti.



#### Passaggio 7

*ad admin1* visualizza uno spazio tra il nome e il cognome. Se non viene risolto, l'accesso non riesce. Questo errore viene lasciato per scopi dimostrativi. Non lasciare spazio qui! L'esempio *admin2* è corretto.

Per visualizzarlo, fare clic con il pulsante destro del mouse sul nome utente *admin 1* e selezionare l'opzione **Proprietà**. Passare quindi alla scheda **Oggetto** per visualizzare il *nome canonico dei* dettagli *dell'oggetto*.

ad admin1 Prop	erties		?	× Se	adadmin2 P	roperties				?	$\times$
Security Remote Des	Environment ktop Services Profile	Sessions CDM+	Remote control Attribute Editor	n U	Security Remote	Er Desktop Se	vironment ervices Profile	Sess	ions DM+	Remote co Attribute E	ntrol ditor
General Ad Published Certifi	dress Account cates Member Of	Profile Tele Password Repl	ephones Organizati ication Dial-in Obj	tion U ject U	General Published C	Address ertificates	Account Member Of	Profile Passwor	Telephone: d Replication	: Organ Dial-in	ization Object
Canonical nam sbcslab.local/ Object class:	e of object: Users/ad admin1 User			] U U U U	Canonical sbcslab.lo Object clas	name of ob cal/Users/a ss: Us	iect adadmin2 ser				

Èinoltre possibile verificare i dettagli *Domain Users* e *RemoteAdmin* per tali nomi utente passando alla scheda *Membro di* sotto l'**opzione Proprietà**.



Passare alla scheda Editor attributi per verificare i valori DistinguishedName per tali nomi utente.

General       Address       Account       Profile       Telephones       Organization         Published Certificates       Member Of       Password Replication       Dial-in       Object         Remote Desktop Services Profile       COM+       Attribute Editor       Published Certificates       Member Of       Password Replication         Attributes:		sions Re	Sess	vironment	En	Security	ntrol U	emote con	ns R	Sessi	vironment	En	Security
Published Certificates       Member Of       Password Replication       Dial-in       Object         Remote Desktop Services Profile       COM+       Attribute Editor       Remote Desktop Services Profile       COM+         Attributes:	Organizati	Telephones	Profile	Account	Address	eneral	nization l	Organi	Telephones	Profile	Account	Address	General
Remote Desktop Services Profile       CDM+       Attribute Editor       U       Remote Desktop Services Profile       CDM+         Attributes:	Dial-in Obi	d Replication	Passwor	Member Of	ificates	blished Ce	Object	Dial-in	Replication	Password	Member Of	Certificates	ublished C
Attributes:       value       Attributes:         ribute       Value       Value         partmentNumber       (not set)       stopProfile       (not set)         sktopProfile       (not set)       spartment       (not set)         stinationIndicator       (not set)       spartmentNumber       (not set)         playName       ad admin1       stinationIndicator       (not set)         playNamePrintable       (not set)       stinationIndicator       (not set)         tinguishedName       CN=ad admin1,CN=Users,DC=sbcslab,DC=local       U       stinationIndicator       (not set)         tinguishedName       Cnot set>       U       stinguishedName       CN=adadmin2,CN=Users,DC=sbcslab         tinguishedName       (not set)       U       stinguishedName       CN=adadmin2	Attribute Editor	.0M+ A'	C	rvices Profile	esktop Se	Remote D	ditor (	Attribute Ed	/+ A	CC	rvices Profile	Desktop Se	Remote
ribute       Value       Value         partmentNumber       (not set)         scription       (not set)         sktopProfile       (not set)         stinationIndicator       (not set)         stinationIndicator       (not set)         playName       ad admin1         playNamePrintable       (not set)         stinguishedName       CN=ad admin1,CN=Users,DC=sbcslab,DC=local         tion       triot cot         ASignature       (not set)         corePropagationD       0x0 = ( )         namicLDAPServer       (not set)         ployeeID       (not set)         ployeeVumber       (not set)         ployeeID       (not set)         <						ttributes:	(						Attributes:
partmentNumber         ifaultClassStore            scription         ifaultClassStore             sktopProfile          ifaultClassStore	^			Value		ibute	^ U				Value		ribute
scription          partment                     >partment          >partment         >partment         >partment         >partment         >partment         >partment         >partment         >partment         >partment         >partment         >partment         >partment         >partment         >partment         >partment         >partment         >partment         >partment         >partment         >partment         >>partment         >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>				<not set=""></not>	ore	aultClassSl	- L				<not set=""></not>	lumber	partmentN
sktopProfile <not set="">         stinationIndicator       <not set="">         playName       ad admin1         playNamePrintable       <not set="">         itigguishedName       CN=ad admin1,CN=Users,DC=sbcslab,DC=local         itigguishedName       CN=ad admin1,CN=Users,DC=sbcslab,DC=local         itigguishedName       <not set="">         ASignature       <not set="">         corePropagationD       0x0 = ( )         namicLDAPServer       <not set="">         ployeeID       <not set="">         ployeeID       <not set="">         vision       <not set="">         vision</not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not>				<not set=""></not>		partment					<not set=""></not>		scription
stinationIndicator <not set="">         iplayName       ad admin1         iplayNamePrintable       <not set="">         itiguishedName       CN=ad admin1,CN=Users,DC=sbcslab,DC=local         itiguishedName       CN=ad admin1,CN=Users,DC=sbcslab,DC=local         itiguishedName       <not set="">         ASignature       <not set="">         CorePropagationD       0x0 = ( )         namicLDAPServer       <not set="">         iployeeID       <not set="">         iployeeID       <not set="">         iployeeIV       <not set=""></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not>				<not set=""></not>	mber	partmentNu					<not set=""></not>	ile	sktopProfi
playName       ad admin1         playNamePrintable <not set="">         itinguishedName       CN=ad admin1,CN=Users,DC=sbcslab,DC=local         itinguishedName       CN=ad admin1,CN=Users,DC=sbcslab,DC=local         itinguishedName       <not set="">         ASignature       <not set="">         CorePropagationD       0x0 = ( )         namicLDAPServer       <not set="">         iployeeID       <not set="">         iployeeID       <not set="">         iployeeIV       <not set=""></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not>				<not set=""></not>		cription					<not set=""></not>	ndicator	stinationIn
playNamePrintable <not set="">         utinguishedName       CN=ad admin1,CN=Users,DC=sbcslab,DC=local         time       <not set="">         ASignature       <not set="">         CorePropagationD       0x0 = ( )         namicLDAPServer       <not set="">         ployeeID       <not set="">         uployeeID       <not set="">         uployeeIVumber       <not set=""></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not>				<not set=""></not>		ktopProfile	L L				ad admin1		:playName
tinguishedName       CN=ad admin1,CN=Users,DC=sbcslab,DC=local       U       splayName       adadmin2         tinguishedName       (not set)       splayName       adadmin2         ASignature       (not set)       stinguishedName       CN=adadmin2,CN=Users,DC=sbcslab         CorePropagationD       0x0 = ( )       stinguishedName       CN=adadmin2,CN=Users,DC=sbcslab         namicLDAPServer       (not set)       U       sSignature       (not set)         uployeeID       (not set)       U       SCrePropagationD       0x0 = ( )         uployeeNumber       (not set)       U       "mamicLDAPServer"       (not set)         uployeeType       (not set)       U       "mamicLDAPServer"       (not set)				<not set=""></not>	cator	tinationInd	l				<not set=""></not>	Printable	playName
ision     isolavNamePrintable     (not set)       ASignature <not set="">        CorePropagationD     0x0 = ( )        namicLDAPServer     <not set="">       uployeeID     <not set="">       uployeeNumber     <not set="">       uployeeType     <not set=""></not></not></not></not></not>				adadmin2		olayName	l l	DC=local	,DC=sbcslab,	1,CN=Use	CN=ad admir	dName	tinguished
ASignature <not set="">       U       stinguishedName       CN=adadmin2,CN=Users,DC=sbcslai         CorePropagationD       0x0 = ( )       U       vision       <not set="">         ployeeID       <not set="">       U       SCorePropagationD       0x0 = ( )         ployeeNumber       <not set="">       U       SCorePropagationD       0x0 = ( )         ployeeType       <not set="">       U       manicLDAPServer       <not set=""></not></not></not></not></not></not>				<not set=""></not>	intable	olavNameF	<b></b> U	_			1101-000		
CorePropagationD     0x0 = ( )     U     vision     Cnock set/       namicLDAPServer <not <="" set="" td="">     U     jASignature     <not <="" set="" td="">       uployeeID     <not <="" set="" td="">     U     iCorePropagationD     0x0 = ( )       uployeeNumber     <not <="" set="" td="">     U     inamicLDAPServer     <not <="" set="" td="">       uployeeType     <not <="" set="" td="">     U     inamicLDAPServer     <not <="" set="" td=""></not></not></not></not></not></not></not>	DC=local	ers,DC=sbcslab,f	2,CN=Use	CN=adadmin/	ame	inguishedN	- L				<not set=""></not>	re	ASignatur
namicLDAPServer <not set="">     U     \$ASignature     <not set="">       iployeeID     <not set="">     U     \$CorePropagationD     0x0 = ()       iployeeNumber     <not set="">     U     inamicLDAPServer     <not set="">       iployeeType     <not set="">     U     inamicLDAPServer     <not set=""></not></not></not></not></not></not></not>	_			CHOC SEC/		sion	ι ι				0x0 = ( )	agationD	CorePropa
uployeeID <not set="">     uployeeNumber     CorePropagationD     0x0 = ( )       uployeeNumber     <not set="">     uployeeNumber     <not set="">       uployeeType     <not set="">     uployeeID     <not set=""></not></not></not></not></not>				<not set=""></not>		ASignature					<not set=""></not>	PServer	namicLDA
ployeeNumber <not set=""></not>				0x0 = ( )	ationD	CorePropa					<not set=""></not>		ployeelD
ployeeType <not set=""></not>				<not set=""></not>	Server	amicLDAF					<not set=""></not>	imber	ployeeNu
	~			<not set=""></not>		ploveeID	v .				<not set=""></not>	ре	nployeeT yr
	>					<		>					<
					_		i		_				

## Passaggio 8

Eseguire l'accesso con il *nome di accesso utente*, in questo caso *admin2*, significa che l'accesso è riuscito.

## Passaggio 9

Èpossibile visualizzare i dettagli sull'acquisizione dei pacchetti come mostrato nella schermata seguente.

	Capturing from E	hernet			– 🗆 X	
File	Edit View	io Capture Ana	lyze Statistics .	Telephony	Wireless Tools Help	
Æ.	<b>i</b> 🧕 🧾		⊨ ⇔ ≅ T 🕹		Q, Q, Q, II	
	dap				Expression	ŀ
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_	
1	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 result]	
	2856 329 897	172 16 1 126	172 16 1 2	LDAP	61 uphindRequest(3)	
	2050 525.057	172.10.1.120	172.10.1.2	LUAP	or anornered as ( )	
						~
>	Erame 2855• 20	6 hytes on wire	(1648 hits) 3	206 hvter	cantured (1648 hits) on interface 0	-
5	Ethernet II, S	rc: Microsof_01	:7e:01 (00:15:5	5d:01:7e:	(1), Dst: (isc. 44:57:7f (e:bd:14:457:7f)	
> :	Internet Proto	col Version 4,	Src: 172.16.1.2	2, Dst: 1	72.16.1.126	
2	Transmission C	ontrol Protocol	, Src Port: 389	9, Dst Po	rt: 59096, Seq: 23, Ack: 135, Len: 152	
Ľ	> LDAPMessage	searchResEntry	2) "CN=adadmin	12.CN=Use	rs,DC=sbcslab,DC=local" [1 result]	
<b>v</b> 1	Lightweight Di	rectory Access 1	Protocol			
	> LDAPMessage	searchResDone(2	2) success [1 r	result]		

## Cosa succede se non si estrae lo spazio dal campo del nome completo?

Se si tenta di utilizzare il *nome di accesso dell'utente,* in questo caso *admin*, si noterà che l'accesso non riesce in quanto il server LDAP (Lightweight Directory Access Protocol) non può restituire l'oggetto perché il *nome completo,* in questo caso, *ad admin1,* ha uno spazio. Sarà possibile visualizzare questi dettagli durante l'acquisizione dei pacchetti, come mostrato nella schermata seguente.

## Conclusioni

Èstato completato ed evitato un errore di accesso per l'autenticazione remota tramite Active Directory su RV34x Router.