لوخدلا ليجست تاداشراو دعب نع ةقداصملا و RV34x و Active Directory تاهجوم مادختساب

فدەلا

مادختساب دعب نع ةقداصملا نيوكت ةيفيك لاقملا اذه حرشي Windows Active Directory (AD) مادختساب دعب نع ةقداصمل نيوك بنجتل تامولعملا ريفوت متيس ،كلذ ىلإ ةفاضإلاب .Cisco RV34x قلسلس تاهجوم ىلع لوخدلا ليجست يف لمتحم أطخ ثودح.

ەمدقملا

.يجراخ ةقداصم بولسأ ديدحت كمزلي ،RV34x هجوملا ىلع ةمدخلا ةقداصم تادادعإ نيوكت دنع

يه RV34x ةلسلسل نم مجوم ىلع قيجراخلا تانايبلا قدعاق قيولوأ نوكت ،يضارتفا لكشب قمدخ مدختستسف ،مجوملا ىلع RADIUS مداخ قفاضإب تمق اذإ RADIUS/LDAP/AD/Local. ققداصمل قيجراخلا RADIUS تانايب قدعاق ىرخألا تامدخلاو بيولا ىلإ لوخدلا ليجست امدحو بيو ىلإ لوخدلا ليجست قمدخل قيجراخ تانايب قدعاق نيكمتل رايخ دجوي ال .مدختسمل ،مجوملا ىلع منيكمتو RADIUS عاشنإ درجمبو .ىرخأ قمدخل ىرخأ تانايب قدعاق نيوكتو ،بيولا ىلإ لوخدلا ليجستل قيجراخ تانايب قدعاق مرخألا تامدخلاو بيولا ال مدختسمل من (VPN) قيرهاظلا قصاخلا قكبشلاو ،عقوم ملا عقوم نم (VPN) قيرهاظلا قصاخلا قكبشلاو تنم (VPN) قيرهاظلا قصاخلا قلابشلاو ،عقوم ملا عقوم نم (VPN) قيرهاظلا قصاخلا قلاب ماد 2001 ال المراح الي المراح ال المراح ال الماد الماد الماد الماد ماد الماد الم

عيمج نيزختب AD موقي .ةيلخاد AD ةمدخ Microsoft رفوت ،Windows مدختست تنك اذا مدختسي .تاسايسلاو ةزهجألاو نيمدختسملا كلذيف امب ةكبشلل ةيساسألا تامولعمل دراوم مادختساب لمعلا لهسي وهو .اهتراداو ةكبشلا ءاشنإل دحاو ناكمك AD نولوؤسملا .قدحوم ةقيرطب ةعونتملاو ةدقعملاو ةطبارتملا ةكبشلا

دوجوملا) يجراخلا AD رايخ مادختساب ةقداصملا هل حرصم صخش يأل نكمي ،اهنيوكت درجمبو نكمي RV34x هجوم ىلع ةنيعم ةمدخ يأ مادختسال (Windows Server ليغشت ماظن يف ةزهجألا ىلع نورفوتي مەنأ املاط ،ةرفوتملا تازيملا مادختسإ نيدمتعملا نيمدختسملل ةقداصملا نم عونلا اذه مادختسال ةبولطملا جماربلاو.

جماربلا رادصٳ | قيبطتلل ةلباقلا ةزهجألا

- RV340 | 1.0.03.16
- RV340W | 1.0.03.16
- RV345 | 1.0.03.16
- ارطلا RV345P | 1.0.03.16 زارطل

تايوتحملا لودج

- <u>زيممِلا مِسالاً ةمِيق يلع فرعتلاً</u> •
- <u>المctive Directory ل نيمدختسم ةعومجم ءاشنا</u>
- مجوم ا ىل Active Directory ليصافت ةفاضا RV34x
- <u>الماكلام مسالا لقح نم محاسملا نخات مل انا ثدحي انام</u>

زيمملا مسالا ةميق ىلع فرعتلا

ي*مدختس*م ةرادإ ةهجاو ىلإ لوصولا Active Directory يمدختسم ةرادإ ةهجاو ىلإ لوصولا Windows 2016. .**صﺉاصځلا** حتفا مث ،سواملا قوف نميألا سواملا رزب رقنا مث ،**نيمدختسملا** قيواح دلجم ددح *مدختسملا ةيواح راس*م لقح يف اقحال اهمادختسإ متيس يتلا DistinguishedName ةميق ظحال هجومل RV34x.



Active Directory ل نيمدختسم ةعومجم ءاشنإ

1 ةوطخلا

تاعومجم < ماظنلاا نيوكت ىلإ لقتنا .RV34x ةلسلسلا نم مجوم ىلإ لوخدلا ليجستب مق نيمدختسملا.



.**دئاز ةنوقيأ** ىلع رقنا



3 ةوطخلا

.**قبطي** ةقطقط .*ةعومجم مسا* لخدأ

RV345P-RV345P	English 🔹 😯 🚺 🕩
User Groups	2 Apply Cancel
Group Name: RemoteAdmin	

نيمدختسم ةعومجم ءاشنإ مت ،لاثملا اذه يف RemoteAdmin.

4 ةوطخلا

ريرحتلا ةنوقيأ رقنا .ةديدجلا نيمدختسملا ةعومجمل ةرواجملا رايتخالا ةناخ قوف رقنا.



Services Web Login/NETCONF/RESTCONF O Disabled O Read Only O Administrator Site to Site VPN

6 ةوطخلا

.**قبطي** ةقطقط



7 ةوطخلا

لوؤسملا تازايتماب رەظت يتلا ةدىدجلا نيمدختسملا ةعومجم نآلا دەاشتس.

		E	cisco R	V345P-router4491EF				cisco (admir	English	• 🕜 (0 0
⊗ €	Getting Started Status and Statistics	Use	er Groups						A	pply	Cancel
**	Administration	Use	er Groups Table								^
*	System Conliguration		• 🕜 🖻								
	System	C	Group 🗢	Web Login/NETCONF/RESTCONF \$	S2S-VPN \$	EzVPN/3rd Party 🗢	SSL VPN \$	PPTP 🗢	L2TP 🖨	802.1x 🖨	;
	Time		RemoteAdmin	Admin	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	
	log	_									· ·
			admin	Admin	Disabled	Disabled	SSLVPNDef	Enabled	Enabled	Enabled	
	Email		admin anyconnect	Admin Disabled	Disabled Disabled	Disabled	SSLVPNDef	Enabled Disabled	Enabled Disabled	Enabled Disabled	

RV34x ەجوملا ىلع Active Directory ليصافت ةفاضإ

1 ةوطخلا

ريرحتلا ةنوقيأ رقناو *AD* رايخ ددح **.نيمدختسملا تاباسح < ماظنلا نيوكت** ىلإ لقتنا مداخل ليصافت ةفاضإل AD.

		E	cisco	RV345P-route	er4491EF	[💾 cisco (admin)	English 🔹 ?	0 🕩						
⊗	Getting Started	Use	r Accou	nts				Apply	Cancel						
•	Status and Statistics														
**	Administration	* Shou	* Should have at least one account in the "admin" group												
۰ (System Configuration		Remote Authentication Service												
	System 1	Ren													
	Time	Ren	Remote Authentication Service Table												
	Log	4+													
	Email	0	Enable \$	Name 🗢	Primary Server 🗢	1	Backup Server 🗢								
(User Accounts 2	G	0	AD 3											
	User Groups			LDAP											
	IP Address Groups	0	0	RADIUS											
	SNMP														
	Discovery-Bonjour	* Pleas	se input remo	e authentication se	ervice configurations when it is enabled.										

2 ةوطخلا

ةقطقط .م*دختسملا ةيواح راسم*و *ذفنمل*او *يساسأل*ا مد*اخل*او *نالعإلا لاجم مسا*ليصافت لخدأ ق**بطي**.



يف Windows مداخ نم ةطقتلملا *مدختسملا ةيواح راسم* ليصافت لاخدا يل جاتحت :**قظحالم** قلاقملا هذه يف <mark>قزيمملا مسالا قميق يلع فرعتل.</mark> مسق.

ية ليصافتالا ، لافت *cn=user، dc=sbcslab، dc=local.* ين المتسال المتسال الذه يف وه (LDAP) ليلدلل لوصولل فيفخلا لوكوتوربال مداخل

3 ةوطخلا

نيمدختسملا ةعومجم مسا قباطت اەنأو ،*نيمدختسملا ةعومجم* نيوكت نم ققحت ،نالعإلا يف ەجوملل.

File Action Media Clipboard View Help		
≞ © • ⊚ ⊍ Ⅱ ► ₅ > ≝		
Active Directory Users and Computers File Action View Help	i 🐍 🔌 în 🍸 🗾 🍬	– – ×
 Active Directory Users and Computers [sbcslabfores Saved Queries Sbcslab.local Builtin Computers Domain Controllers ForeignSecurityPrincipals Keys LostAndFound Managed Service Accounts Program Data System Users NTDS Quotas TPM Devices 	Name Enterprise Read-only Domain Controllers Group Policy Creator Owners Group Policy Creator Owners Group Policy Creator Owners Creation Controllers Experimental Stream S	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
	Schema Admins	Security Group - Universal

4 ةوطخلا

متيس ،*ةلئاعلا مسا* و *ىلوألا فورحلا ،لوألا مسالا* ةئبعتب مق ،مدختسم - ديدج نئاك تحت ةلئاعلا مساو لوألا مسالا نيب ةفاسم راهظإ عم ،ايئاقلت *لماكلا مسالا* لقح علم.

متي نل وأ *لماكلا مسالا* عبرم يف ريخألا مسالاو لوألا مسالا نيب ةفاسملا فذح بجي حيحص لكشب لوخدلا ليجست. اەفذح بجي يتلا لماكلا مسالا يف ةحاسملا ةروصلا ەذە ضرعت:



5 ةوطخلا

يأ ةلازاب *لماكلا مسالا* لقح ليدعت ىلإ جاتحت ،ىرخأ ةرم .رخآ مدختسم ءاشنإل تاوطخلا ررك ءاشنا ءاەناب مق مث رورملا ةملك دادعإل **يلاتلا** قوف رقنا .ايئاقلت اەۋاشنا مت تافاسم مدختسملا.

ةحيحصلا ةقيرطلا يه هذه .لماكلا مسالا يف ةحاسملا فذح مت هنأ ةروصلا هذه حضوت مدختسملا ةفاضإل:



اثيدح اهتفاضإ تمت يتلا مدختسملا ليصافت نم لك نيمدختسملا ةمئاق رهظت.



7 ةوطخلا

اذه نكي مل اذإ ،ةلئاعلاا مساو لوألاا مسالا نيب ةفاسم رهظي *نالعإلا لوؤس*م نأ ظحالتس كرتت ال ،يحيضوتلا ضرعلا ضارغال أطخلا اذه كرت متي .لوخدلا ليجست لشفيس ،اتباث لاثم !كانه ةحاسملا.

مث .**صئاصخلا** رايخ ددجو ad admin 1 مدختسم مسا قوف نميألا سواملا رزب رقنا ،ضرعلل *نئاكلا* ليصافتل *ميلع فراعتملا مسالا* ىرتل **نئاك** بيوبتلا ةمالع ىلإ لقتنا.

ad admin1 Pro	perties				?	×	Se Se	adadmin2 F	Properties				?	\times
Security Remote De	Security Environment Sessions Remote Desktop Services Profile COM+		Remote control Attribute Editor			Security Environment Remote Desktop Services Profile			Sessions F		Remote co Attribute E	ntrol ditor		
General / Published Cert Canonical na sbcslab.loca Object class:	Address ificates ime of obje il/Users/a Use	Account Member Of ect: d admin1	Profile Password	Teleph d Replica	iones Or tion Dial-ir	ganization Object		General Published (Canonical sbcslab.k Object cla	Address Dertificates Loame of ob ocal/Users/ ass: U	Account Member Of hiect adadmin2	Profile Passwor	Telephone d Replication	es Organ Dial-in	Disation Object

ءامسأب ةصاخلا *RemoteAdmin*و *لاجملا يمدختس*م ليصافت نم ققحتلا كنكمي امك رايخلا نمض بيوبتلا ةمالع *وضع* ىلإ لاقتنالا لالخ نم هذه نيمدختسملا

ad admin1 Propertie	S		?	× S	adadmin2 Pr	operties					?	×
Security	Remote contro	ol U	Security	Er	vironment	Sessions		Remote co		ontrol		
General Address	Services Profile	CUM+ Profile Teleph	Attribute Edito ones Organizat	tion U	General	Desktop Se Address	Account Member Of	Profile	CM+ Teleph	A iones	ttribute t Orga	Editor nization
Member of:	, manber of	rassword neplical	on Diahin Ol		Member of:	ertificates	Member of	rasswo	ro Replica	aon	Diann	Ubject
Name	Active Directo	ry Domain Services	Folder	U	Name		Active Directo	ry Domai	n Services	s Folde	ar -	
Domain Users	sbcslab.local/	Users		U	Domain U	sers	sbcslab.local/	Users				
RemoteAdmin	sbcslab.local/	Users		U	RemoteAd	dmin	sbcslab.local/	Users				

ةصاخلا DistinguishedName ميق نم ققحتلل *تامسلا ررحم* بيوبتلا ةمالع ىلإ لقتنا ەذە نيمدختسملا ءامسأب.

l admin1 l	Properties				?	\times	S	adadmin2 F	Properti	es			?	>
Security	Er	vironment	Sess	ions	Remote	control	U	Security		Environment	Ses	sions f	Remote cont	trol
General	Address	Account	Profile	Telephon	es Org	anization	U	General	Addre	ess Account	Profile	Telephones	Organiz	zatio
Published C	Certificates	Member Of	Passwor	d Replication	n Dial-in	Object	U	Published (Certificat	es Member Of	Passwo	d Replication	Dial-in C	Obie
Remote	Desktop Se	ervices Profile	C	OM+	Attribute	Editor	U	Remote	Deskto	p Services Profile	0	OM+	Attribute Edi	itor
Attributes:							U	Attributes:						
:ribute		Value				^	U	tribute		Value			1	^
partmentN	lumber	<not set=""></not>					U	faultClass	Store	<not set=""></not>				
scription		<not set=""></not>					U	partment		<not set=""></not>				
sktopProfi	ile	<not set=""></not>						partment	Number	<not set=""></not>				
stinationIn	ndicator	<not set=""></not>					ŭ	escription		<not set=""></not>				
:playName	•	ad admin1						esktopPro	file	<not set=""></not>				
playName:	Printable	<not set=""></not>					U	estination	ndicator	<not set=""></not>				
tinguished	dName	CN=ad admir	n1,CN=Use	ers,DC=sbcsl	lab,DC=loo	al	U	splayNam	е	adadmin2				
		that add					U	splayNam	ePrintab	le <not set=""></not>			_	
ASignatur	е	<not set=""></not>					U	stinguishe	dName	CN=adadmi	in 2, CN=Us	ers,DC=sbcslab	,DC=local	
CoreProp	agationD	0x0 = ()					U	VISION		CHOC3EC/			_	
namicLDA	PServer	<not set=""></not>					U	SASignatu	Ire	<not set=""></not>				
ployeeID		<not set=""></not>						CoreProp	agation	D 0x0 = ()				
ployeeNu	mber	<not set=""></not>					U U	namicLD/	APServe	er <not set=""></not>				
ployeeT y	ре	<not set=""></not>				~		nployeeID		<not set=""></not>			•	~
<						>	U	<					>	
Edit					Filte	ſ	U	Edit				[Filter	

8 ةوطخلا

ةلاحلا هذه يفو ،*مدختسملا لوخد ليجست مسا* مادختساب لوخدلا ليجستب مق، adadmin2، حجان لوخدلا ليجست نأ ىرتس.

9 ةوطخلا

ةيلاتلا ةشاشلا ةطقل يف حضوم وه امك ةمزحلا طاقتلا لوح ليصافتلا ةيؤر كنكمي.

4	🖸 Capturing from Ethernet – 🗆 🗙											
Fi	le Edi	t View	Go Capture Ana	lyze Statistics	Telephony	Wireless Tools Help						
1		5 💿 🗌		⇔⇔≌₹₫		Q. Q. Q. II						
	ldap						Expression	. +				
No		Time	Source	Destination	Protocol	Lengt Info		^				
	2093	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 ma	at_				
	2851	1 329.849	_ 172.16.1.126	172.16.1.2	LDAP	99 bindRequest(1) "adadmin2@SBCSLAB.LOCAL" simple						
	2852	2 329.883	172.16.1.2	172.16.1.126	LDAP	76 bindResponse(1) success						
-	2854	1 329.883	172.16.1.126	172.16.1.2	LDAP	143 searchRequest(2) "cn=adadmin2,cn=Users,dc=sbcslab,dc=local" wholeSubtree						
	2855	5 329.896	_ 172.16.1.2	172.16.1.126	LDAP	206 searchResEntry(2) "CN=adadmin2,CN=Users,DC=sbcslab,DC=local" searchResDone(2) success [1 re	sult]					
	2856	5 329.897	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: Nicrosof_01:7e:01 (00:15:5d:01:7e:01), Dst: Cisco_44:57:7f (ec:bd:ld:44:57:7f) > Internet Protocol Version 4, Src: 172.16.1.2, Dst: 172.16.1.126 > Transmission Control Protocol, Src Port: 389, Dst Port: 59096, Seq: 23, Ack: 135, Len: 152 > Lightweight Directory Access Protocol											
Ļ	> LD Light > LD	APMessag weight D APMessag	e searchResEntry irectory Access e searchResDone((2) "CN=adadmir Protocol 2) success [1 r	n2,CN=Use result]	rs,DC=sbcslab,DC=local" [1 result]						

؟لماكلا مسالا لقح نم ةحاسملا ذخأت مل اذإ ثدحي اذام

ليجست نأ ىرتس ،adadmin قلاحلا هذه يف *،مدختسملا لوخد ليجست مسا* مادختسا تلواح اذا عاجرا هنكمي ال (LDAP) نزولا فيفخ ليلدلا ىلا لوصولا لوكوتورب مداخ نأل لشفي لوخدلا قيؤر ىلع ارداق نوكتس .ةحاسم هب *،ad admin1 و ،*قلاحلا هذه يف *،لماكلا مسالا* نأل نئاكلا .قيار عام الحال الماليا قطقل يف حضوم وه امك مزحلا طاقتلا دنع ليصافتلا كلت

رارقلا

دعب نع ةقداصملا يف لشف ثودح تبنجتو حاجنب لوخدلا ليجست لامكا نم نآلا تيهتنا دقل ربع Active Directory مجوملا ىلع RV34x.

ةمجرتاا مذه لوح

تمجرت Cisco تايان تايانق تال نم قعومجم مادختساب دنتسمل اذه Cisco تمجرت ملاعل العامي عيمج يف نيم دختسمل لمعد يوتحم ميدقت لقيرشبل و امك ققيقد نوكت نل قيل قمجرت لضفاً نأ قظعالم يجرُي .قصاخل امهتغلب Cisco ياخت .فرتحم مجرتم اممدقي يتل القيفارت عال قمجرت اعم ل احل اوه يل إ أم اد عوجرل اب يصوُتو تامجرت الاذة ققد نع اهتي لوئسم Systems الما يا إ أم الا عنه يل الان الانتيام الال الانتيال الانت الما