Autenticación remota y guía de inicio de sesión mediante routers Active Directory y RV34x

Objetivo

En este artículo se explica cómo configurar la autenticación remota mediante Windows Active Directory (AD) en los Cisco RV34x Series Routers. Además, se proporcionará información para evitar un posible error de inicio de sesión.

Introducción

Cuando configura los parámetros de autenticación de servicio en el router RV34x, debe seleccionar un método de autenticación externo.

De forma predeterminada, la prioridad de la base de datos externa en el router serie RV34x es RADIUS/LDAP/AD/Local. Si agrega el servidor RADIUS en el router, el servicio de inicio de sesión web y otros servicios utilizarán la base de datos externa RADIUS para autenticar al usuario. No hay ninguna opción para habilitar una base de datos externa para el servicio de inicio de sesión web solo y configurar otra base de datos para otro servicio. Una vez que se crea RADIUS y se habilita en el router, el router utilizará el servicio RADIUS como base de datos externa para el inicio de sesión web, VPN de sitio a sitio, VPN EzVPN/de terceros, VPN SSL, VPN PPTP/L2TP y 802.1x.

Si utiliza Windows, Microsoft proporciona un servicio AD interno. AD almacena toda la información esencial para la red, incluidos los usuarios, los dispositivos y las políticas. Los administradores utilizan AD como un único lugar para crear y administrar la red. Facilita el trabajo con recursos de red diferentes, complejos e interconectados de forma unificada.

Una vez configurada, cualquier persona autorizada puede autenticarse usando la opción AD externa (presente en el sistema operativo del servidor Windows) para utilizar cualquier servicio específico en el router RV34x. Los usuarios autorizados pueden utilizar las funciones proporcionadas, siempre que dispongan del hardware y el software necesarios para utilizar ese tipo de autenticación.

Dispositivos aplicables | Versión de software

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

Table Of Contents

- Identificar el valor de nombre distinguido
- <u>Crear un grupo de usuarios para Active Directory</u>
- <u>Agregar detalles de Active Directory en el router RV34x</u>
- ¿Qué sucede si no quita el espacio del campo de nombre completo?

Identificar el valor de nombre distinguido

Acceda a la interfaz de administración *Usuarios y equipos de Active Directory* en el servidor Windows 2016. Seleccione la carpeta del contenedor **Users**, haga clic con el botón derecho del ratón y abra **Properties**. Tenga en cuenta el valor *DistinguishedName* que se utilizará más adelante en el campo *User Container Path* del router RV34x.



Crear un grupo de usuarios para Active Directory

Paso 1

Inicie sesión en el router de la serie RV34x. Vaya a **Configuración del sistema > Grupos de usuarios**.



Haga clic en el icono más.



Paso 3

Introduzca un nombre de grupo. Haga clic en Apply (Aplicar).



En este ejemplo, se ha creado un grupo de usuarios RemoteAdmin.

Paso 4

Haga clic en la casilla de verificación junto al nuevo grupo de usuarios. Haga clic en el **icono de** edición.



Paso 5

Desplácese hacia abajo por la página hasta *Services*. Haga clic en el botón de opción Administrator.







Paso 6

Haga clic en Apply (Aplicar).



Paso 7

Ahora verá el nuevo grupo de usuarios mostrándose con privilegios de administrador.

		E	cisco R	V345P-router4491EF				cisco (admin	Englist		
⊗	Getting Started	Use	r Groups						Ap	ply Ca	ancel
Ģ	Status and Statistics								_		
**	Administration	Use	r Groups Table								^
۰	System Configuration										
	System		Group 🗢	Web Login/NETCONF/RESTCONF 🖨	S2S-VPN \$	EzVPN/3rd Party €				000 4	
							SSE VEN V	PPIP ¥	L2IP ╤	802.1x ⊊	
	lime		RemoteAdmin	Admin	Disabled	Disabled	Disabled	Disabled	Disabled	B02.1x ₽	
	Time Log		RemoteAdmin admin	Admin Admin	Disabled Disabled	Disabled Disabled	Disabled SSLVPNDef	Disabled Enabled	Disabled Enabled	B02.1x ≑ Disabled Enabled	
	lime Log Email		RemoteAdmin admin anyconnect	Admin Admin Disabled	Disabled Disabled Disabled	Disabled Disabled Disabled	Disabled SSLVPNDef SSLVPNDef	Disabled Enabled Disabled	Disabled Enabled Disabled	Disabled Disabled Disabled	

Agregar detalles de Active Directory en el router RV34x

Paso 1

Vaya a **Configuración del sistema > Cuentas de usuario.** Seleccione la opción *AD* y haga clic en el **icono de edición** para agregar los detalles para el servidor AD.

		E	.ılı.ılı. cısco	RV345P-rout	iter4491EF	0	💾 cisco (admin)	English 🔹 ?	() ()
⊗ 	Getting Started Status and Statistics	Use	er Accou	nts				Apply	Cancel
**	Administration	* Shou	uld have at lea	st one account in	the "admin" group				
•	System Configuration System	Ren	note Aut	henticatior					
	Time	Ren	note Authent	cation Service Ta	- Table				^
	Log	4+	@ 1						
	Email	0	Enable \$	Name 🗢	Primary Server 🗢	E	Backup Server 🗢		
(User Accounts 2	G	0	AD 3					
	User Groups			LDAP					
	IP Address Groups	0		RADIUS					
	SNMP								
	Discovery-Bonjour	* Pleas	se input remo	te authentication s	service configurations when it is enabled.				

Paso 2

Ingrese los detalles *AD Domain Name*, *Primary Server*, *Port* y *User Container Path*. Haga clic en Apply (Aplicar).



Nota: Debe ingresar los detalles de *la ruta de contención de usuario* capturados del servidor de Windows en la sección <u>Identificar el valor de nombre distinguido</u> de este artículo.

En este ejemplo, los detalles son *Cn=user,dc=sbcslab,dc=local*. El puerto de escucha predeterminado del servidor LDAP es 389.

Paso 3

En AD, verifique que el *grupo de usuarios* esté configurado y coincida con el *nombre de grupo de usuarios* del router.

b 🕘 💿 🥥 💵 🕨 🔂 🎐 🖳		
Active Directory Users and Computers File Action View Help		– o x
◆ ⇒ 2 🗊 4 🗉 🗙 🖾 😖 🖬 🖬	🐍 🗽 🗊 🍸 🚨 🐍	
 Active Directory Users and Computers [sbcslabfores Saved Queries Saved Queries Solutin 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 Guest Key Admins krbtgt L2TP User1 L2TPVPN PPTP User1 PTPVPN Priv15 admin Priv15 admin Priv15 Admins RAS and IAS Servers RAS and IAS Servers Read-only Domain Controllers RemoteAdmin SBCS admin sbcs labadmin1 sbcsadlabadmin1	Type Security Group - Universal Security Group - Global User Security Group - Global User User Security Group - Global User Security Group - Global Security Group - Global

Paso 4

En New Object - User, rellene *First name*, *Initials* y *Last name*, el campo *Full name* se rellenará automáticamente, mostrando un espacio entre el nombre y los apellidos.

El espacio entre el nombre y los apellidos en el cuadro *Nombre completo* debe eliminarse o no se iniciará sesión correctamente.

Esta imagen muestra el espacio en el nombre completo que se debe eliminar:



Paso 5

Repita los pasos para crear otro usuario. Una vez más, debe modificar el campo *Full Name* quitando los espacios creados automáticamente. Haga clic en **Next** para configurar la contraseña y finalizar la creación del usuario.

Esta imagen muestra que se eliminó el espacio en el nombre completo. Esta es la forma correcta de agregar el usuario:



La lista Usuarios mostrará los dos detalles de usuario recién agregados.



Paso 7

Observará que el *anuncio admin1* muestra un espacio entre el nombre y los apellidos, si esto no se corrige, el login fallará. Este error se está dejando para fines de demostración, no deje el espacio ahí! El ejemplo *adadmin2* es correcto.

Para ver, haga clic con el botón derecho en el nombre de usuario *ad admin 1* y seleccione la opción **Properties**. A continuación, vaya a la ficha **Object** para ver los detalles *Canónicos de Object*.

ad admin1 Pro	perties		? ×	Se Se	adadmin2 Pro	operties				?	\times
Security	Environment	Remote control	U	Security Environment			Sess	ions F	Remote control		
Remote De	sktop Services Profile	Attribute Editor	U	Remote Desktop Services Profile				OM+	Attribute Editor		
General Address Account Published Certificates Member Of		Profile Telep	hones Organization	U	General	Address	Account	Profile	Telephones	Organi	zation
		Password Replic	ation Dial-in Object	U	Published Cer	rtificates	Member Of	Passwor	d Replication	Dial-in	Object
Canonical nar sbcslab.local Object class:	me of object: /Users/ad admin1 User			U U U U	Canonical n sbcslab.loca Object class	ame of obi al/Users/a : Us	adadmin2				

Además, puede verificar los detalles *Domain Users* y *RemoteAdmin* para esos nombres de usuario navegando a la pestaña *Member Of* bajo la opción *Properties*.



Navegue hasta *la* ficha *Editor de atributos* para verificar los valores *DistinguishedName* para esos nombres de usuario.

d admin1 Pr	operties					?	\times	s ad	ladmin2 P	ropert	ties					?	×
Security	Er	nvironment	Sess	ions	Rem	ote contro	l	U	Security		Er	vironment	Ses	sions	Remo	te cor	ntrol
General	Address	Account	Profile	Teleph	nones	Organizat	tion	U	General	Addr	ess	Account	Profile	Telephon	es (Organi	zatio
Published Certificates		Member Of	Passwor	d Replica	ation Di	al-in Ob	iect	UF	Published (Certifica	ites	Member Of	Passwor	d Replication	n Dia	-in	Obie
Remote D	esktop Se	ervices Profile	C	OM+	Attri	bute Editor	r	U	Remote	Deskto	op Se	rvices Profile	C	OM+	Attrib	ute E c	litor
Attributes:								U	Attributes:								
ribute		Value				^		U	tribute			Value					^
partmentNu	mber	<not set=""></not>				- 14		U	aultClass	Store		<not set=""></not>					
scription		<not set=""></not>						U.	partment			<not set=""></not>					
sktopProfile		<not set=""></not>						Ŭ.	partment	Vumber	r	<not set=""></not>					
stinationIndi	icator	<not set=""></not>							escription			<not set=""></not>					
:playName		ad admin1							sktopProl	file		<not set=""></not>					
:playNamePr	rintable	<not set=""></not>						U	stination	ndicato	r	<not set=""></not>					
:tinguishedN	lame	CN=ad admir	n1,CN=Use	ers,DC=sb	boslab,DC	=local		U	splayNam	е		adadmin2					
		that acts				-		U	splayNam	ePrintal	ble	<not set=""></not>				_	
ASignature		<not set=""></not>						U	stinguishe	dName	;	CN=adadmir	n2,CN=Use	ers,DC=sbcsl	ab,DC=	local	н
CorePropag	gationD	0x0 = ()						U	VISION			KHOUSE(2				-	
namicLDAP	Server	<not set=""></not>						u	ASignatu	re		<not set=""></not>					
ployeeID		<not set=""></not>						-	CoreProp	agation	nD	0x0 = ()					
ployeeNum	ber	<not set=""></not>							namicLD/	- APServ	/er	<not set=""></not>					
ployeeType	•	<not set=""></not>				\sim			nployeeID			<not set=""></not>					~
<						>		U	<							>	
Edit						Filter]	UUU	Edit						F	ïlter	

Paso 8

Inicie sesión con el *nombre de inicio de sesión del usuario*, en este caso, *adadmin2*, verá que el login es exitoso.

Paso 9

Puede ver los detalles de la captura de paquetes como se muestra en la siguiente captura de pantalla.

4	Capturing from Ethernet —										
Fi	e Edit	t View Go	o Capture Ana	lyze Statistics	Telephony	Wireless Tools Help					
1				⇔ ⇒ ≌ T J		Q. Q. Q. III					
	ldap					🛛 🖘 💌 Expression	+				
No		Time	Source	Destination	Protocol	Lengt Info	^				
	2097	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 mat	t_				
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_	172.16.1.126	172.16.1.2	LDAP	143 searchRequest(2) "cn=adadmin2,cn=Users,dc=sbcslab,dc=local" wholeSubtree					
t											
	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), 2	206 bytes	captured (1648 bits) on interface 0					
>	Ether	net II, Sr	c: Microsof_01	:7e:01 (00:15:	5d:01:7e:	01), Dst: Cisco_44:57:7f (ec:bd:1d:44:57:7f)					
>	Inter	net Protoc	ol Version 4,	Src: 172.16.1.2	2, Dst: 1	72.16.1.126					
2	Trans	mission Co	ntrol Protocol	, Src Port: 389	9, Dst Po	rt: 59096, Seq: 23, Ack: 135, Len: 152					
ľ	> LD	Weight Dir APMessage	ectory access i searchResEntry	(2) "CN=adadmir	12.CN=Use	rs.DC=shcslab.DC=local" [1 result]					
÷	Light	weight Dir	ectory Access	Protocol							

¿Qué sucede si no quita el espacio del campo de nombre completo?

Si intenta utilizar el *nombre de inicio de sesión de usuario,* en este caso *adadmin*, verá que el inicio de sesión falla porque el servidor LDAP (protocolo ligero de acceso a directorios) no puede devolver el objeto porque *Nombre completo*, en este caso, *ad admin1,* tiene un espacio. Podrá ver esos detalles al capturar los paquetes como se muestra en la siguiente captura de pantalla.

Conclusión

Ya ha completado correctamente y evitado un inicio de sesión fallido para la autenticación remota a través de Active Directory en el router RV34x.