Guide d'authentification et de connexion à distance à l'aide des routeurs Active Directory et RV34x

Objectif

Cet article explique comment configurer l'authentification à distance à l'aide de Windows Active Directory (AD) sur les routeurs de la gamme Cisco RV34x. En outre, des informations seront fournies pour éviter une erreur de connexion potentielle.

Introduction

Lorsque vous configurez les paramètres d'authentification de service sur le routeur RV34x, vous devez sélectionner une méthode d'authentification externe.

Par défaut, la priorité de base de données externe sur le routeur de la gamme RV34x est RADIUS/LDAP/AD/Local. Si vous ajoutez le serveur RADIUS sur le routeur, le service de connexion Web et d'autres services utiliseront la base de données externe RADIUS pour authentifier l'utilisateur. Il n'existe aucune option permettant d'activer une base de données externe pour le service de connexion Web seul et de configurer une autre base de données pour un autre service. Une fois RADIUS créé et activé sur le routeur, le routeur utilise le service RADIUS comme base de données externe pour la connexion Web, le VPN site à site, le VPN EzVPN/tiers, le VPN SSL, le VPN PPTP/L2TP et 802.1x.

Si vous utilisez Windows, Microsoft fournit un service AD interne. AD stocke toutes les informations essentielles pour le réseau, y compris les utilisateurs, les périphériques et les politiques. Les administrateurs utilisent AD en tant qu'emplacement unique pour créer et gérer le réseau. Il facilite l'utilisation de ressources réseau interconnectées, complexes et différentes de manière unifiée.

Une fois configuré, toute personne autorisée peut s'authentifier à l'aide de l'option AD externe (présente dans le système d'exploitation Windows Server) pour utiliser n'importe quel service spécifique sur le routeur RV34x. Les utilisateurs autorisés peuvent utiliser les fonctionnalités fournies, à condition qu'ils disposent du matériel et du logiciel nécessaires pour utiliser ce type d'authentification.

Périphériques pertinents | Version du logiciel

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

Table des matières

- Identifier la valeur du nom distinctif
- Créer un groupe d'utilisateurs pour Active Directory
- Ajouter des détails Active Directory sur le routeur RV34x
- Que se passe-t-il si vous ne retirez pas l'espace du champ de nom complet ?

Identifier la valeur du nom distinctif

Accédez à l'interface de gestion *Utilisateurs et ordinateurs Active Directory* sur le serveur Windows 2016. Sélectionnez le dossier du conteneur **Utilisateurs**, cliquez avec le bouton droit de la souris et ouvrez **Propriétés**. Prenez note de la valeur *DistinguishedName* qui sera utilisée ultérieurement dans le champ *User Container Path* du routeur RV34x.



Créer un groupe d'utilisateurs pour Active Directory

Étape 1

Connectez-vous au routeur de la gamme RV34x. Accédez à **Configuration système > Groupes** d'utilisateurs.



Étape 2

Cliquez sur l'icône plus.



Étape 3

Entrez un nom de groupe. Cliquez sur Apply.

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

Dans cet exemple, un groupe d'utilisateurs RemoteAdmin a été créé.

Étape 4

Cochez la case en regard du nouveau groupe d'utilisateurs. Cliquez sur l'icône de modification.



Étape 5

Faites défiler la page vers le bas jusqu'à Services. Cliquez sur la case d'option Administrateur.

Services



Étape 6

Cliquez sur Apply.



Étape 7

Le nouveau groupe d'utilisateurs s'affiche avec les privilèges d'administrateur.

		•	cisco	V345P-router4491EF				cisco (admin) English	• • •	0
\otimes	Getting Started	Us	ser Groups						A	oply	Cancel
¢	Status and Statistics										
**	Administration	ι	Jser Groups Table								^
٥	System Configuration		1 🕫 🖨								
	System		Group 🗢	Web Login/NETCONF/RESTCONF \$	S2S-VPN \$	EzVPN/3rd Party 🗢	SSL VPN \$	PPTP 🗢	L2TP 🗢	802.1x 🖨	
	System Time	(□ Group ≑□ RemoteAdmin	Web Login/NETCONF/RESTCONF \$	S2S-VPN \$	EzVPN/3rd Party \$	SSL VPN \$	PPTP 🗢 Disabled	L2TP \$ Disabled	802.1x ≎ Disabled	
	System Time Log	(Group \$ RemoteAdmin admin 	Web Login/NETCONF/RESTCONF \$ Admin Admin	S2S-VPN ¢ Disabled Disabled	EzVPN/3rd Party Disabled Disabled	SSL VPN \$ Disabled SSLVPNDef	PPTP 🖨 Disabled Enabled	L2TP \$ Disabled Enabled	802.1x \$ Disabled Enabled]
	System Time Log Email	(Group \$ RemoteAdmin admin anyconnect 	Web Login/NETCONF/RESTCONF ¢ Admin Admin Disabled	S2S-VPN \$ Disabled Disabled Disabled	EzVPN/3rd Party \$ Disabled Disabled Disabled	SSL VPN \$ Disabled SSLVPNDef	PPTP \$ Disabled Enabled Disabled	L2TP ¢ Disabled Enabled Disabled	802.1x Disabled Enabled Disabled)
	System Time Log Email User Accounts	(Group \$ RemoteAdmin admin anyconnect guest 	Web Login/NETCONF/RESTCONF ¢ Admin Admin Disabled Disabled	S2S-VPN \$	EzVPN/3rd Party \$ Disabled Disabled Disabled Disabled	SSL VPN \$ Disabled SSLVPNDef Disabled	PPTP \$ Disabled Enabled Disabled Disabled	L2TP \$ Disabled Enabled Disabled Disabled	802.1x ¢ Disabled Enabled Disabled Disabled)

Ajouter des détails Active Directory sur le routeur RV34x

Étape 1

Accédez à **Configuration système > Comptes d'utilisateurs.** Sélectionnez l'option *AD* et cliquez sur l'**icône de modification** pour ajouter les détails du serveur AD.

		E	cisco	RV345P-route	ter4491EF	6	cisco (admin)	English 🔹 ?	() ()
\otimes	Getting Started	Usei	r Accou	nts				Apply	Cancel
•	Status and Statistics								
쓭	Administration	* Shoul	ld have at lea	st one account in t	the "admin" group				
\$ (System Configuration System	Rem	iote Aut	hentication	n Service				
	Time	Rem	ote Authenti	cation Service Ta	able				^
	Log	4+							
	Email		Enable \$	Name 🗢	Primary Server 🗢	E	Backup Server 🗢		
(User Accounts 2	e	0	AD 3					
	User Groups	0	0	LDAP					
	IP Address Groups	0	0	RADIUS					
	SNMP								
	Discovery-Bonjour	* Pleas	e input remo	e authentication se	service configurations when it is enabled.				

Étape 2

Entrez les détails AD Domain Name, Primary Server, Port et User Container Path. Cliquez sur Apply.



Note: Vous devez entrer les détails du *chemin du conteneur utilisateur* capturés à partir du serveur Windows dans la section <u>Identifier la valeur du nom distinctif</u> de cet article.

Dans cet exemple, les détails sont *Cn=user, dc=sbcslab, dc=local*. Le port d'écoute par défaut du serveur LDAP (Lightweight Directory Access Protocol) est 389.

Étape 3

Dans l'AD, vérifiez que le *groupe d'utilisateurs* est configuré et qu'il correspond au nom *du groupe d'utilisateurs* du routeur.



Étape 4

Sous New Object - User, entrez *First name*, *Initials* and *Last name*, le *Full name* sera automatiquement renseigné, indiquant un espace entre le prénom et le nom.

L'espace entre le prénom et le nom dans la zone *Nom complet* doit être supprimé ou il ne se connectera pas correctement.

Cette image montre l'espace dans le nom complet qui doit être supprimé :



Étape 5

Répétez les étapes pour créer un autre utilisateur. Une fois de plus, vous devez modifier le champ *Nom complet* en supprimant les espaces créés automatiquement. Cliquez sur **Suivant** pour configurer le mot de passe et terminer la création de l'utilisateur.

Cette image montre que l'espace du nom complet a été supprimé. Voici la bonne façon d'ajouter l'utilisateur :



La liste Utilisateurs affiche les deux détails des utilisateurs nouvellement ajoutés.



Étape 7

Vous remarquerez que l'*ad admin1* affiche un espace entre le prénom et le nom de famille, si ce n'est pas corrigé, la connexion échouera. Cette erreur est laissée à des fins de démonstration, ne laissez pas l'espace là! L'exemple *admin2* est correct.

Pour afficher, cliquez avec le bouton droit de la souris sur le nom d'utilisateur *admin 1 de l'annonce* et sélectionnez l'option **Propriétés**. Ensuite, accédez à l'onglet **Objet** pour afficher le *nom canonique des* détails *de l'objet*.

ad admin1 Prop	perties			?	×	Se	adadmin2 P	roperties				?	\times	
Security Remote Des	Security Environment Sessions Remote Desktop Services Profile COM+			Remote control Attribute Editor			Security Environment Remote Desktop Services Profile			Sessions Remote of COM+ Attribute			control e Editor	
General Ar Published Certif Canonical nan sbcslab.local	ddress Account icates Member Of ne of object: /Users/ad admin1	Profile Te Password Re	elephones plication	Organizat Dial-in Ob	ject		General Published C Canonical sbcslab.lo	Address Certificates name of of ocal/Users/	Account Member Of hiect adadmin2	Profile Passwor	Telephon d Replication	es Organ n Dial-in	Dization Object	
Object class:	User					U	Object cla	ss: U	ser					

Vous pouvez également vérifier les détails *Domain Users* et *RemoteAdmin* pour ces noms d'utilisateur en accédant à l'onglet *Member Of* sous l'option **Properties**.



Accédez à l'onglet Éditeur d'attributs pour vérifier les valeurs DistinguishedName pour ces noms d'utilisateur.

d admin1 f	Properties					?	×	S	adadmin2 P	rope	erties					?	2
Security	Er	nvironment	Sess	ions	Ren	note conti	rol	U	Security		E	nvironment	Ses	sions	B	emote co	ntrol
General	Address	Account	Profile	Teleph	nones	Organiz	ation	U	General	Ad	dress	Account	Profile	Telep	hones	Organ	nizatio
Published Certificates Member Of Password Replic			d Replica	tion D	ial-in 0)biect	U	Published 0	Certific	cates	Member Of	Passwo	rd Replic	ation	Dial-in	Obie	
Remote	Desktop Se	ervices Profile	C	DM+	Attr	ribute Edit	tor	U	Remote	Desk	ktop S	ervices Profile	0	:ОМ+	A	ttribute E	ditor
Attributes:								U	Attributes:								
:ribute		Value				^	•	U	tribute			Value					^
partmentN	lumber	<not set=""></not>						U	aultClass	Store	э	<not set=""></not>					
scription		<not set=""></not>						υ	partment			<not set=""></not>					
sktopProfi	ile	<not set=""></not>						- i	partment	Numb)er	<not set=""></not>					
stinationIn	ndicator	<not set=""></not>						l ü	escription			<not set=""></not>					
playName		ad admin1							esktopProl	file		<not set=""></not>					
:playName	Printable	<not set=""></not>						U	estination	ndica	itor	<not set=""></not>					
tinguished	dName	CN=ad admir	n1,CN=Use	ers,DC=sb	ocslab,D1	C=local		U	splayNam	е		adadmin2					
		includi:				-		U	splayNam	ePrint	table	<not set=""></not>					
ASignatur	re	<not set=""></not>						U	stinguishe	dNan	ne	CN=adadmir	2,CN=Us	ers,DC=:	sboslab,	DC=local	
CoreProp	agationD	0x0 = ()						U	VISION			CHOC SEC/					
namicLDA	PServer	<not set=""></not>						υ	SASignatu	re		<not set=""></not>					
nployeeID		<not set=""></not>						— н	CoreProp	agati	ionD	0x0 = ()					
ployeeNu	ımber	<not set=""></not>						i i	namicLD/	APSe	rver	<not set=""></not>					
ployeeT y	pe	<not set=""></not>				~	1	l .	nployeeID			<not set=""></not>					¥
<						>		l .	<							>	
Edit						Filter		U U	Edit							Filter	

Étape 8

Connectez-vous avec le *nom de connexion de l'utilisateur*, dans ce cas, *admin2*, vous verrez que la connexion a réussi.

Étape 9

Vous pouvez voir les détails de la capture de paquets comme indiqué dans la capture d'écran suivante.

	Capturing from Ethernet —										
Fi	le Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help										
1				⊨ ⇔ ≌ 🖣 🕹		Q. Q. Q. III					
	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	-				
	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					
ł											
	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)					
	2030		1/1110111110	1/11101111	LUHI	or anotheredgese(a)					
							~				
>	Frame	2855: 206	hytes on wire	(1648 hits), (06 hytes	cantured (1648 hits) on interface 0	_				
>	Ether	net II, Sr	c: Microsof_01	:7e:01 (00:15:5	5d:01:7e:	(a), Dst: (isco.44:57:7f (ec:bd:1d:44:57:7f)					
>	Inter	net Protoc	ol Version 4, S	Src: 172.16.1.2	2, Dst: 1	72.16.1.126					
>	Trans	mission Co	ntrol Protocol	, Src Port: 389	9, Dst Po	rt: 59096, Seq: 23, Ack: 135, Len: 152					
ľ	Light	weight Dir	ectory Access F	Protocol	2 CN-Use	ne Discherlah Dislocal" [1 norult]					
Ļ	Light	weight Dir	ectory Access F	Protocol	iz jeni-Ose	syc-sucside ju-ideal [1 + care]					

Que se passe-t-il si vous ne retirez pas l'espace du champ de nom complet ?

Si vous essayez d'utiliser le *nom de connexion utilisateur,* dans ce cas *admin*, vous verrez que la connexion échoue car le serveur LDAP (Lightweight Directory Access Protocol) ne peut pas renvoyer d'objet car *Full name,* dans ce cas, *ad admin1,* a un espace. Vous pourrez voir ces détails lors de la capture des paquets, comme indiqué sur la capture d'écran suivante.

Conclusion

Vous avez maintenant réussi et évité une connexion échouée pour l'authentification à distance via Active Directory sur le routeur RV34x.