Ejemplo de Configuración de Autenticación de Usuario VPN ASA contra Servidor NPS de Windows 2008 (Active Directory) con RADIUS

Contenido

Introducción Prerequisites Requirements Componentes Utilizados Configurar Diagrama de la red Configuraciones Configuración de ASDM Configuración de CLI Windows 2008 Server con configuración de NPS Verificación Depuraciones de ASA Troubleshoot

Introducción

Este documento explica cómo configurar un dispositivo de seguridad adaptable (ASA) para comunicarse con un servidor de políticas de red (NPS) de Microsoft Windows 2008 con el protocolo RADIUS de modo que los usuarios WebVPN heredados de Cisco VPN Client/AnyConnect/Clientless WebVPN se autentiquen con Active Directory. NPS es una de las funciones de servidor que ofrece Windows 2008 Server. Es equivalente a Windows 2003 Server, IAS (Internet Authentication Service), que es la implementación de un servidor RADIUS para proporcionar autenticación de usuario de marcado remoto. De manera similar, en Windows 2008 Server, NPS es la implementación de un servidor RADIUS para proporcionar autenticación de un servidor RADIUS. Básicamente, ASA es un cliente RADIUS a un servidor RADIUS NPS. ASA envía solicitudes de autenticación RADIUS en nombre de los usuarios de VPN y NPS las autentica con Active Directory.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

ASA que ejecuta la versión 9.1(4)

• Servidor Windows 2008 R2 con servicios de Active Directory y función NPS instalada The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configurar

Nota: Use la <u>Command Lookup Tool (clientes registrados solamente) para obtener más</u> información sobre los comandos usados en esta sección.

Diagrama de la red



Configuraciones

Configuración de ASDM

- 1. Elija el grupo de túnel para el que se requiere autenticación NPS.
- 2. Haga clic en Editar y elija Básico.
- 3. En la sección Autenticación, haga clic en Administrar.

-Advanced		TEST	
-Advanced	Aliases:	TEST	
	Authentication		
	Method:	AAA Certificate Both	\frown
	AAA Server Group:	LOCAL	Manage
		Use LOCAL if Server Group fails	\bigcirc
	Client Address Assignment –		
	DHCP Servers:		
		None OHCP Link OHCP Subnet	
	Client Address Pools:	test	Select
	Client IPv6 Address Pools:		Select
		IPv6 address pool is only supported for SSL.	
	Default Group Policy		
	Group Policy:	DfltGrpPolicy	✓ Manage
	(Following field is an attribu	ute of the group policy selected above.)	
	Enable SSL VPN dien	t protocol	
	Enable IPsec(IKEv2)	client protocol	
	DNS Servers: 10.40.	3.10	
	WINS Servers:		
	Domain Name: hk.intr	axa	

- 4. En la sección AAA Server Groups , haga clic en Add.
- 5. En el campo AAA Server Group (Grupo de servidores AAA), introduzca el nombre del grupo de servidores (por ejemplo, NPS).
- 6. En la lista desplegable Protocol , elija RADIUS.
- 7. Click

OK.

A Server Groups								-
erver Group	Protocol	Accounting Mode	Reactivation Mode	Dead Time	Max Failed Attempt	5		Add
ICAL	LOCAL							Edit
nd	001	Match Case	Add AAA Serve AAA Server Group: Protocol: Accounting Node:	r Group NFS RADOUS () Smultz	• menus @ Single			Delete
ivers in the Select	ed Group		Reactivation Modes	Depiet	ion 🔿 Timed			
erver Name or IP A	vddress Interfac	te Timeout	Max Faleri Attenni	10 10	a cons			Add
			E Duable interior		data			Edit
				errors and obs	ua le			Delete
			Chable Active C	krectory Agen	it mode			Move Up
			VOID Compat	hilty Online				Move Down
			OK	Car	ncel Hellp			Test
ndt	001	Match Case						
DAP Attribute F	tap							(8
				- C	Apply Res	et		

- 8. En la sección Servidores de la sección Grupo Seleccionado, elija el Grupo de Servidor AAA agregado y haga clic en **Agregar**.
- 9. En el campo Server Name (Nombre de servidor) o IP Address (Dirección IP), introduzca la dirección IP del servidor.
- 10. En el campo Server Secret Key (Clave secreta del servidor), introduzca la clave secreta.
- 11. Deje los campos Server Authentication Port y Server Accounting Port en el valor predeterminado a menos que el servidor escuche en un puerto diferente.
- 12. Click OK.
- 13. Click
 - OK.

dvanced	Name:	TEST					Edit AA	A Server		
	Analytic.	16.71								
	Authenticate	on					Server Gro	NUP:	NPS	
configure AAA Ser	rver Groups		a contract of	-		22	Interface	Name:	inside +	
Ad Server Groups							Server Na	ne or IP Address:	10.105.130.51	
www.server.orsups							Timeout:		10 seconds	
Server Group	Protocol	Accounting Mode	Reactivation Mode	Dead Time	Max Pailed Attempts	Aod				
OCAL	LOCAL	- Contraction	Receiver and the second se			Edit	RADIUS PI	s anetera	C	
953	RADIUS	ange	Depletion	110	- P		Server J	Authentication Port	1645	
						Delete	Server J	Accounting Port:	1646	
Pind:	0 01	Match Case					Retry In	derval:	10 seconds	
ervers in the Select	ted Group					-	Server 3	ecret Key:		
					- (A44	Common	Password:		
Server Name or IP	Address interfac	tureeut 3				74040			F	
						\sim	ACL Net	mask Convert:	Standard	-
39.105.130.51	nade	30				Edit	ACL Net	mask Convert:	Standard	•
0.105.130.51	insde	23				Edit	ACL Net Microsof	mask Convert: It CHAPv2 Capable	Standard	•
00.105.130.51	Inside	33				Edit Delete	ACL Net Microsol SDI Messa	mask Convert: It CHAPv2 Capable ges	Standard	•
0, 105, 110, 51	Insde	38				Edit Delete Nove Up	ACL Net Microsoft SDI Messa Messa	maak Convert: 1 OHAPv2 Capable ges age Table	Standard	•
00, 005, 100, 91	jenside	90				Edit Delete Move Up Hove Down	ACL Net Microsof SDI Messa Messa Messa	maak Convert: It CHAPv2 Capable ges age Table age Name	Standard	•
0, 105, 110, 91	jenside	98				Edit Delete Move Up Move Down	ACL Net Microsoft SDI Messa Messa Messa ready	mask Convert: It CHAPv2 Capable ges age Table age Name -for-sys-pin	Standard V Message Text ACCEPT A SYSTEM	enerated PI
0.005.130.51	inside	33				Edit Delete Move Up Move Down Test	ACL Net Microsoft SDI Messa Mess ready new s	maak Convert: ht CHAPv2 Capable ges age Table age Name -for-sys-pin sin-reenter	Standard Wessage Text ACCEPT A SYSTEM Reenter PIN:	GENERATED PJ
60 2015 1200 51	lesde	Match Case				Edit Delete Move Up Move Down Test	ACL Net Microsoft SDI Messa Micss Ress ress ress ress ress	maak Convert: ht CHAPv2 Capable ges age Table age Name Hor-sys-pin ain-reenter ain-reenter ain-meth	Standard Standard Message Text ACCEPT A SYSTEM CREMETE PIN: Do you want to ento	er your own pit
5md:		Match Case				Edit Delete Nove Up Move Down Test	ACL Net Microsoft SDI Messa Pless ready news news news news	mask Convert: tt CHAPv2 Capable ges age Table age Name -for-sys-pin sin-reenter sin-reenter sin-reenter sin-reenter sin-reenter	Standard Standard Message Text ACCEPT A SYSTEM Reenter PIN: Do you want to ento new PIN with the n	GENERATED PI er your own pir
Find:	Inside O O I Map	Match Case				Edit Delete Move Up Move Down Test	ACL Net Microsoft SDI Messa Pless ready news news news news	maak Convert: t CHAPv2 Capable ges age Table age Name -for-sys-pin ain-reeth sin-reeth coode-and-reauth coode	Standard Standard Message Text ACCEPT A SYSTEM Reenter PIN: Do you want to enb Enter Next PASCO	GENERATED PJ er your own pir ext card code tot
n dis 19031	Inside S O I Map	Match Case				Edit Delese Move Up Move Down Test	ACL Net Vicrosol SCI Messa Mess ready new ready new ready new ready new ready	mask Convert: t CHAPv2 Capable ges ges Table age Name -for-sys-pin ain-reenter ain-meth ccode-and-reauth ccode ain-spo-ok	Standard Standard Message Text ACCEPT A SYSTEM Do you want to ento new PDI with the m Terter Next PASSCO New PDI Accepted New PDI Accepted	GENERATED PI er your own pir ext card code tot
Find:	irode 0 0 1 Hap	Match Case	Cancel	Help		Edit Delete Move Up Move Down Test	AC, Net Vicrosoft SEE Messa Pessa ready new - new - new - new - new - new - new -	mask Convert: tt CHAPv2 Capable ges age Table age Name -for-sys-pin ain-reenter in-reenter in-reenter in-reenter in-reenter in-sys-ok in-sys-ok in-sys-ok	Standard Standard Message Text ACCEPT A SYSTEM Reenter PIN new PIN with the ne Enter Next PASSCO New PIN Accepted Please nemeble ty Enter wave new Male	GENERATED P1 er your own pir ext card code top our new PfN ha de marcel PfN
ind: DAP Attribute (kada O O I	Match Case	Cancel	Help		Edit Delete Move Up Move Down Test	AC, Net Vicrocol SDE Hessa Pless ready new i new i ne	mask Convert: tt CHAPv2 Capable ges age Table age Name -for sys-pin in-reentler sin-setter sin-setter sin-setter sin-setter sin-setter sin-setter sin-setter sin-setter sin-setter	Standard Message Text ACCEPT A SYSTEM Reenter PIN: Do you want to ent new PIN with the n Enter Next PASSOO New PIN Accepted Please remember yo Enter your new Api	GENERATED P3 er your own pir ext card code sce our new P0N ha-Numerical P1
Find:	krode 0 © 1 Map	Match Case	Cancel	Help		Edit Delete Move Up Move Down Test	AC, Net Vicrocol SDE Hessa Pess ready net net net net net net net net net net	mask Convert: tt CHAPv2 Capable ges age Table age Name -for-sys-pin in-reentler in-reentler in-reentler in-reentler in-reentler in-sys-ok in-sys-ok in-sys-ok in-sys in-ree e-dick in a text cel	Standard Standard Message Text ACCEPT A SYSTEM ACCEPT A SYSTEM Reenter PIN: Do you want to end new PIN with the n Enter Next PASSOO New PIN Accepted Please remember yo Enter your new Api to make changes.)	GENERATED PD er your own pin ext card code loci our new PIN ha-Numerical PI
Find:	iroid: Map	Match Case	Cancel	Help		Edit Delese Move Up Move Down Test	AC, Net Vicrosof SEE Messa Pess ready net - net - net - net - net - net - net - net - Doub	mask Convert: th CHAPv2 Capable ges	Standard Message Text Message Text ACCEPT A SYSTEM Do you want to ento new PDI with the m Triter Next PASSCO New PDI Accepted Please remember yo Enter your next Abi to make changes.) e default message texts.	er your own pir er your own pir ext card code lot our new PIN ha-Numerical PI

14. En la lista desplegable Grupo de servidores AAA, elija el grupo (NPS en este ejemplo) agregado en los pasos anteriores.

15. Click

OK.

Advanced Alases: TEST Authentication Method:	Basic	Name:	TEST	
Authentication Method:	Advanced	Aliases:	TEST	
Method:		Authentication		
AAA Server Group: NPS Manage Use LOCAL if Server Group fails Client Address Assignment DHCP Servers: None DHCP Link DHCP Subnet Client Address Pools: test Select Client IPv6 Address Pools: Select Default Group Policy Group Policy: DftGrpPolicy Manage (Folowing field is an attribute of the group policy selected above.) Client protocol DNS Servers: 10.40.3.10 WINS Servers: 10.40.3.10 WINS Servers: Domain Name:		Method:	AAA Certificate Both	
□ Use LOCAL if Server Group fails Client Address Assignment DHCP Servers:		AAA Server Group:	NPS V	Manage
Client Address Assignment DHCP Servers: None DHCP Link DHCP Subnet Client Address Pools: test Select Client IPv6 Address Pools: Select Default Group Policy Group Policy: DftGrpPolicy Manage (Following field is an attribute of the group policy selected above.) Cholowing field is an attribute of the group policy selected above.) Cholowing field is an attribute of the group policy selected above.) Cholowing field is an attribute of the group policy selected above.) Cholowing field is an attribute of the group policy selected above.) Cholowing field is an attribute of the group policy selected above.) Cholowing field is an attribute of the group policy selected above.) Cholowing Servers: Domain Name: Domain Name:			Use LOCAL if Server Group fails	
DHCP Servers: Image: Client Address Pools: test Select Client IPv6 Address Pools: Image: Client Select Select Default Group Policy Image: Client Select Select Group Policy: DftGrpPolicy Image: Client Select Group Policy: Image: Client Group Policy Image: Client Group Policy Group Policy: Image: Client Group Policy Image: Client Group Policy Group Policy: Image: Client Group Policy Image: Client Group Policy Group Policy: Image: Client Group Policy Image: Client Group Policy Group Policy: Image: Client Group Policy Image: Client Group Policy Group Policy: Image: Client Group Policy Group Policy Selected above.) Image: Client Group Policy Image: Client Group Policy: Image: Client Group Policy Image: Client Group Policy Image: Client Group Policy: Image: Client Group Policy Image: Client Group Policy Image: Client Group Policy: Image: Client Group Policy Image: Client Group Policy Image: Client Group Policy: Image: Client Group Policy Image: Client Group Policy Image: Client Group Policy: Image: Client Group Policy Image: Client Group Policy </td <td></td> <td>Client Address Assignment —</td> <td></td> <td></td>		Client Address Assignment —		
None DHCP Link DHCP Subnet Client Address Pools: test Client IPv6 Address Pools: Select Default Group Policy Group Policy: DfltGrpPolicy Manage (Following field is an attribute of the group policy selected above.) Image Image: Disc (IKEv2) client protocol DNS Servers: DNS Servers: 10.40.3.10 Image: Domain Name: Image: Disc (IKEv2)		DHCP Servers:		
Client Address Pools: test Select Client IPv6 Address Pools: Select Default Group Policy Group Policy: DfltGrpPolicy Manage (Following field is an attribute of the group policy selected above.) © Enable SSL VPN client protocol IV Enable IPsec(IKEv2) client protocol DNS Servers: 10.40.3.10 WINS Servers: Domain Name:			None DHCP Link DHCP Subnet	
Client IPv6 Address Pools: Select Default Group Policy Group Policy: DftGrpPolicy Manage (Following field is an attribute of the group policy selected above.) IVE Enable SSL VPN client protocol IVE Enable IPsec(IKEv2) client protocol INS Servers: 10.40.3.10 WINS Servers: Domain Name:		Client Address Pools:	test	Select
Default Group Policy OfftGrpPolicy Manage Group Policy: DfftGrpPolicy Manage (Following field is an attribute of the group policy selected above.) Image: Comparison of the group policy selected above.) Image: Comparison of the group policy selected above. Image: Comparison of the group policy selected above. Image: Comparison of the group policy selected above. Image: Comparison of the group policy selected above. Image: Comparison of the group policy selected above. Image: Comparison of the group policy selected above. Image: Comparison of the group policy selected above. Image: Comparison of the group policy selected above. Image: Comparison of the group policy selected above. Image: Comparison of the group policy selected above. Image: Comparison of the group policy selected above. Image: Comparison of the group policy selected above. Image: Comparison of the group policy selected above. Image: Comparison of the group policy selected above. Image: Comparison of the group policy selected above. Image: Comparison of the group policy selected above. Image: Comparison of the group policy selected above. Image: Comparison of the group policy selected above. Image: Comparison of the group policy selected above. Image: Comparison of the group policy selected above. Image: Comparison of the group policy selected above.		Client IPv6 Address Pools:		Select
Group Policy: DftGrpPolicy Manage (Following field is an attribute of the group policy selected above.) Image: Comparison of the group policy selected above.) Image: Comparison of the group policy selected above. Image: Comparison of the group policy selected above. Image: Comparison of the group policy selected above. Image: Comparison of the group policy selected above. Image: Comparison of the group policy selected above. Image: Comparison of the group policy selected above. Image: Comparison of the group policy selected above. Image: Comparison of the group policy selected above. Image: Comparison of the group policy selected above. Image: Comparison of the group policy selected above. Image: Comparison of the group policy selected above. Image: Comparison of the group policy selected above. Image: Comparison of the group policy selected above. Image: Comparison of the group policy selected above. Image: Comparison of the group policy selected above. Image: Comparison of the group policy selected above. Image: Comparison of the group policy selected above. Image: Comparison of the group policy selected above. Image: Comparison of the group policy selected above. Image: Comparison of the group policy selected above. Image: Comparison of the group policy selected above. Image: Comparison of the group policy selected above. Image: Compar		Default Group Policy		
(Following field is an attribute of the group policy selected above.)		Group Policy:	DfltGrpPolicy 👻	Manage
Image: Construction of the sector of the		(Following field is an attribu	ite of the group policy selected above.)	
Image: Construction of the sector of the		Enable SSL VPN clien	t protocol	
DNS Servers: 10.40.3.10 WINS Servers: Domain Name:		Enable IPsec(IKEv2)	client protocol	
WINS Servers: Domain Name:		DNS Servers: 10.40.	3.10	
Domain Name:		WINS Servers:		
		Domain Name:		
			"	•
< <u> </u>	Find:	O Ne	xt 🔘 Previous	

Configuración de CLI

aaa-server NPS protocol radius aaa-server NPS (inside) host 10.105.130.51 key ***** tunnel-group TEST type remote-access tunnel-group TEST general-attributes address-pool test authentication-server-group (inside) NPS tunnel-group TEST webvpn-attributes group-alias TEST enable

ip local pool test 192.168.1.1-192.168.1.10 mask 255.255.255.0

De forma predeterminada, ASA utiliza el tipo de autenticación del protocolo de autenticación de contraseña (PAP) no cifrado. Esto no significa que el ASA envíe la contraseña en texto sin formato cuando envía el paquete RADIUS REQUEST. Más bien, la contraseña de texto sin formato se cifra con el secreto compartido RADIUS.

Si la administración de contraseñas se habilita bajo el grupo de túnel, ASA utiliza el tipo de autenticación MSCHAP-v2 para cifrar la contraseña de texto sin formato. En tal caso, asegúrese de que la casilla de verificación **Microsoft CHAPv2 Capable** esté marcada en la ventana Edit AAA Server configurada en la sección ASDM configuration.

tunnel-group TEST general-attributes
address-pool test
authentication-server-group (inside) NPS
password-management

Nota: El comando **test aaa-server authentication** siempre utiliza PAP. Sólo cuando un usuario inicia una conexión con un grupo de túnel con la administración de contraseñas habilitada, el ASA utiliza MSCHAP-v2. Además, la opción 'password-management [password-caduc-in-days]' solo se admite con LDAP (protocolo ligero de acceso a directorios). RADIUS no proporciona esta función. Verá la opción de caducidad de la contraseña cuando la contraseña ya haya caducado en Active Directory.

Windows 2008 Server con configuración de NPS

La función de servidor NPS se debe instalar y ejecutar en el servidor de Windows 2008. Si no es así, elija **Inicio > Herramientas administrativas > Roles de servidor > Agregar servicios de rol**. Elija Network Policy Server e instale el software. Una vez instalado el rol de servidor NPS, complete estos pasos para configurar el NPS para aceptar y procesar las solicitudes de autenticación RADIUS del ASA:

 Agregue el ASA como cliente RADIUS en el servidor NPS. Elija Administrative Tools > Network Policy Server .Haga clic con el botón derecho en Clientes RADIUS y elija Nuevo.

🞭 Network Policy	Server					_	
File Action View	w Help						Start
💠 🔿 🔁 📅							
NPS (Local)		RADIUS Clients					
RADIUS Clients a RADIUS Clients a RADIUS Clients Remote RA	New Seport List	RADIUS cl network.	ients allow you to	specify the network acc	cess servers, that	t provide access to your	
Connection	View 🕨	Friendly Name	IP Address	Device Manufacturer	NAP-Capable	Status	
Health Polic	Refresh	Cisco Router	10.105.130.69	RADIUS Standard	No	Enabled	
Accounting	Help						
							« ()
•		•					2:31 AM 7/20/2013
New Network Access	Device						

Introduzca un nombre descriptivo, una dirección (IP o DNS) y un secreto compartido configurados en el

ASA.

Network Policy Server	Cisco Router Properties	×		Chart
File Action View Help	Settings Advanced			J.
NPS (Local)	Provide this RADIOS client			-
RADIUS Clients and Servers	Select an existing template:			
RADIUS Clients			to your	
Remote RADIUS Server Group				
Policies	Name and Address			100
Connection Request Policies	Friendly name:			
Health Policies	Cisco Router			
Network Access Protection	Address (ID as DALS).			
Accounting	Address (iF of DNS).			
Templates Management	10.105.130.65			
Contraction in the second second second	Shared Secret	=		
	Select an existing Shared Secrets template:			
	None			
	To manually type a shared secret click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared secret entered here. Shared secrets are case-sensitive.			
	Confirm shared secret:			
				**
	OK Cancel Apply	-1		(b P
4 F	p			12:02 AM 7/20/2013

Haga clic en la ficha Advanced (Opciones avanzadas).En la lista desplegable Nombre del proveedor, elija **Estándar RADIUS**.Click OK.

 RADIUS Clients and Servers RADIUS Clients Remote RADIUS Server G Policies Network Access Protection Accounting Templates Management Radius Standard for most RADIUS clients, or select the RADIUS client vendor from the list. Vendor name: RADIUS Standard Radius Standard Radius Clients of the Radius client vendor from the list. Vendor name: Radius Standard Radius Clients of the Radius client vendor from the list. Vendor name: Radius Clients Management Radius Client vendor from the list. Vendor name: Radius Client is NAP-capable Radius Client is NAP-capable
OK Cancel

2. Cree una nueva política de solicitud de conexión para los usuarios de VPN. El propósito de la política de solicitud de conexión es especificar si las solicitudes de los clientes RADIUS se procesarán localmente o se reenviarán a los servidores RADIUS remotos. En NPS > Policies, haga clic con el botón derecho del ratón en Connection Request Policies y cree una nueva política.En la lista desplegable Tipo de servidor de acceso a la red, elija Sin especificar.

🐝 Network	test Properties		Start
File Actio	cost roper des		June
(= =) 2	Overview Conditions Setting	38	
NPS (Local)	Policy name:	test	
RADIUS			
RAD	Policy State		
Policies	It enabled, NPS evaluates th	his policy while processing connection requests. If disabled, NPS does not evalue this policy.	
Conr	Policy enabled		
Netv			
Network	Network connection method	d	
Accounti	Select the type of network a type or Vendor specific but	occess server that sends the connection request to NPS. You can select either the network access server nether is required. If your network access server is an 802 1X authenticating switch or wireless access or	in
🛒 Templati	select Unspecified.		
	G Turne of partwork access		
	se Type of Helwork access		
	Unspecified	Ž	
	C Vendor specific:		
	10 🛨		
			-
			**
-			- 7/20/2013
		OK Cancel	/

Haga clic en la pestaña **Condiciones**.Haga clic en Add (Agregar).Introduzca la dirección IP del ASA como condición 'Dirección IPv4 del cliente'.

🗈 Network	a the commentation of the	
Ella Actio	test Properties	Start
	Overview Conditions Settings	長
NPS (Local)	Configure the conditions for this network policy.	
RADIUS	If conditions match the connection request, NPS uses this policy to authorize the connection request. If conditions do not match the connection request, NPS skips this policy and evaluates other policies, if additional policies are configured.	$\mathbf{\Sigma}$
Policies		-
Conr	Condition Value	
📔 Netv	Client IPv4 Address 10.105.130.69	
📔 Heal		
Network		
Accounti		
Template		
	Condition description:	
	The Client IP Address condition specifies the IP address of the RADIUS client that forwarded the connection request to NPS.	
	Add Edt Remov	**
2		10 10
		12:08 AM
•		7/20/2013
2 C	OK Cancel ,	

Haga clic en la pestaña **Settings**.En Forwarding Connection Request , elija **Authentication**. Asegúrese de seleccionar el botón de opción Autenticar solicitudes en este servidor.Click OK.



3. Agregue una política de red donde puede especificar qué usuarios pueden autenticarse.Por ejemplo, puede agregar grupos de usuarios de Active Directory como condición. En esta directiva sólo se autentican los usuarios que pertenecen a un grupo de Windows especificado.En NPS, elija Políticas.Haga clic con el botón derecho del ratón en Directiva de red y cree una nueva política.Asegúrese de seleccionar el botón de opción Conceder acceso.En la lista desplegable Tipo de servidor de acceso a la red, elija Sin especificar.

Jan 166	test Properties	Start
File	Overview Conditions Constraints Settings	
() E	Policy name: test	
R P	Policy State If enabled, NPS evaluates this policy while performing authorization. If disabled, NPS does not evaluate this policy.	
N A	Access Permission If conditions and constraints of the network policy match the connection request, the policy can either grant access or deny access. What is access permission?	
	 Grant access. Grant access if the connection request matches this policy. Deny access. Deny access if the connection request matches this policy. Ignore user account dial-in properties. If the connection request matches the conditions and constraints of this network policy and the policy grants access, perform authorization with network policy only; do not evaluate the dial-in properties of user accounts. 	
	Network connection method Select the type of network access server that sends the connection request to NPS. You can select either the network access server type or Vendor specific, but neither is required. If your network access server is an 802.1X authenticating switch or wireless access point, select Unspecified. Type of network access server: Unspecified	
न	Vendor specific:	**

Haga clic en la pestaña **Condiciones**.Haga clic en Add (Agregar).Introduzca la dirección IP del ASA como condición de dirección IPv4 del cliente.Introduzca el grupo de usuarios de Active Directory que contiene usuarios de VPN.

re the conditions for th	raints Settings is network policy.				
re the conditions for th	is network policy.				
tions match the conne tion request, NPS skip	ction request, NPS uses th s this policy and evaluates	is policy to authorize the connect other policies, if additional polici	ction request. If condition les are configured.	ons do not match the	
and the second	Value				
ondition	CKD/VDM				
ient IPv4 Address	10 105 130 69				
n description:					
ent IP Address condition	in specifies the IP address	of the RADIUS client that forwa	rded the connection re	quest to NPS.	
				1	1 -
			Add	Eda Dama	
			Add	Edit Remo	ove .
			Add	Edit Remo	ove .
	andition ser Groups ient IPv4 Address in description: ant IP Address conditio	andition Value ser Groups SKP\VPN ient IPv4 Address 10.105.130.69	andition Value ser Groups SKP\VPN ient IPv4 Address 10.105.130.69	and tion Value ser Groups SKP\VPN ient IPv4 Address 10.105.130.69	andtion Value ser Groups SKP\VPN ient IPv4 Address 10.105.130.69

Haga clic en la pestaña **Restricciones**.Elija **Métodos de Autenticación**.Asegúrese de que la casilla de verificación Autenticación no cifrada (PAP, SPAP) está marcada.Click OK.

Construction Construints I or	man 1	N 5
Overview Conditions Constraints Se Configure the constraints for this network if all constraints are not matched by the o	tings connection request, network access is denied.	
Constraints: Constraints	May pages ask to these elects that a therefore with the escaliad methods	_
Authentication Methods	Filow access only to those clients that addrendicate with the specified methods.	
Session Timeout	EAP types are negotiated between NPS and the client in the order in which they are listed. EAP Types:	_
Called Station ID	Move Up Move Down	
NAS Port Type		
	Less secure authentication methods:	
	Microsoft Encrypted Authentication Version 2 (MS-CHAP-V2) View can change password after it has expired Microsoft Encrypted Authentication (MS-CHAP)	
	User can change password after it has expired Encrypted authentication (CHAP)	
	Unencrypted authentication (PAP, SPAP) Allow clients to connect without neoptiating an authentication method	
	Perform machine health check only	
1		
	OK Cancel App	

Pasar atributo de política de grupo (atributo 25) desde el servidor RADIUS NPS

Si la política de grupo debe asignarse dinámicamente al usuario con el servidor RADIUS NPS, se puede utilizar el atributo RADIUS de política de grupo (atributo 25).

Complete estos pasos para enviar el atributo RADIUS 25 para la asignación dinámica de una política de grupo al usuario.

 Después de agregar la política de red, haga clic con el botón derecho del ratón en la política de red requerida y haga clic en la ficha Configuración.



 Elija Atributos RADIUS > Estándar. Haga clic en Add (Agregar). Deje el tipo de acceso como Todos.

Network Policy	Server	
File Action VI	est Properties	
(a a) 2 (a)	Overview Conditions Constraints Softings	
NP5 (Local)	Configure the settings for this network policy. If conditions and constraints match the connection request and Patrices	d the policy grants access, settings are applied.
Remot	DADUUS Amiliatus	Add Standard RADIUS Attribute
Policies Conne	RADIUS Attributes To tend additis	To add an attribute to the settings, select the attribute, and then click Add.
Control 10	your RADIUS of	To add a custom or reactational Quocke Spacific attitudada chosa this shalon and caked Yarsho Spacific and than click
📑 Health	Vendor Specific	Add.
Accounting	Network Access Protection	Access type
🗉 🛃 Templates	S NAP Enforcement Attributes:	A1 🔽
	Reference Name	
	Routing and Remote Access Framed Proto	Attributes:
	Allocation Protocol (BAP)	Name
	T IP Filers	Applinterminterval
	- Encounting	Clett
	- IP Settings	FilerId
	gag in storings	Framed AppleTak-Link
	Add	Figured Annial Ski. Zono
		Description
		Specifies the length of the interval (in seconds) between each interim update that the NAS sends
•		
		AddChee
		OK Carel Arde

3. En el cuadro Atributos, elija Clase y haga clic en Agregar. Introduzca el valor del atributo, es decir, el nombre de la política de grupo como cadena. Recuerde que una política de grupo con este nombre debe configurarse en el ASA. Esto es para que el ASA lo asigne a la sesión VPN después de recibir este atributo en la respuesta RADIUS.

Network Policy	r Server test Properties				
Hie Action 0	Dverview Conditions Constraints Settin	ge			
NPS (Local)	Configure the settings for this network policy If conditions and constraints match the con-). rection request and if	he minu manta access sations are annied		
	Sellings		a had Saun accorded to a chicar		
E Policies	RADIUS Attributes	To send addition	Add Standard RADIUS Attribute 🔀 🔀		
Conne Netwo	Standard	Ihen click Edit. I your RADIUS of	To add a custom or predefined Vendor Specific attribute, close this claico and select Vendor Specific, and then click		
🧮 Health E 💺 Network A	Network Access Protection		Add.		
Accounting	S NAP Enforcement	Attributes	Access type:		
an and compared	📳 Extended State	Name	pa 🖂		
	Routing and Remote Access	Service-Type	Allaber		
	Allocation Photocol (BAP)		Acctinerin Interval		
	Financian		Calback Number		
	A IP Sellings		FileNd FramesbandeTink-Link		
		Add	Fremed-AppleTalk-Network		
			Description:		
			Specifies the classification of accounting records.		
•					
			AddUose		
			DK Cancel Apply		
Network Polic	y Server				
Network Polic File Action Vi	x Server Lest Properties	er l			
Network Police File Action Vi	v Server Lest Properties Derview Conditions Constraints Settin Continue the settings for the network polic	gs			
Network Polic File Action Vi NPS (Locel) RADUS CI	x Server Test Properties Overview Conditions Constraints Settin Configue the settings for this network polic If conditions and constraints metch the con	gs) y nection request and (the policy grants access, settings are applied.		
Pie Action Vi	v Server Lest Properties Dverview Conditions Constraints Settin Contigue the estings for this network polic It conditions and constraints match the con Settings Debutts Auchebra	gs y nection request and t	bit Cancel Apply		
Network Police File Action Vi Action Vi Pile Action Pile Action Conne	Server Test Properties Overview Conditions Constraints Settin Configue the settings for this network polic If conditions and constraints match the con Settings: PADIUS Attributes Standard	gs y nection request and f To send addition then click Edit 1	DK Cancel Apply Canc		
	v Server Lest Properties Diverview Conditions Constraints Settin Configue the settings for this network polic If conditions and constraints match the con Settings: RADIUS Attributes Standard Vendor Specific	gs y nection request and t To send addition then click Edit 1 year PADIUS cli	DK Cancel Apply Canc		
	Server Test Properties Overview Conditions Constraints Settin Configue the settings for the network polic If conditions and constraints match the con Settings: RADIUS Attributes Standard Zerverk Access Protection MADE constraints	gs y nection request and t To send additor her click Edit 1 yeur RADIUS cli	DK Cancel Apply DK Cancel Apply C		
Inetwork Police File Action Vi <td>Server Lest Properties Overview Conditions Constraints Settin Configue the satings for this network polic It conditions and constraints match the con Settings: RADIUS Attributes Standard Yendor Specific Network Access Protection NAP Enforcement Evlended State</td> <td>gs y nection request and t To send addition frem click Edit I your FADIUS cli Athibutes: Name</td> <td>DK Cancel Apply Canc</td>	Server Lest Properties Overview Conditions Constraints Settin Configue the satings for this network polic It conditions and constraints match the con Settings: RADIUS Attributes Standard Yendor Specific Network Access Protection NAP Enforcement Evlended State	gs y nection request and t To send addition frem click Edit I your FADIUS cli Athibutes: Name	DK Cancel Apply Canc		
	Server Lest Properties Overview Conditions Constraints Settin Conditions end constraints match the con Settings FADIUS Attributes Standard Yendor Specific Network Access Protection Setting Extended State Routing and Remote Access	gs y nection request and t To send additor then click Edit.1 your PADIUS cli Athibutes: Name FramedProtoc	DK Cancel Apply Canc		
Inetwork Police File Action Vi <td>Server Test Properties Overview Conditions Constraints Settin Configue the settings for this network polic It conditions and constraints match the con- Settings: RADIUS Attributes Settings RADIUS Attributes Standard Vendor Specific Network Access Protection NAP Enforcement Setting and Remote Access Multink and Bandwidth Mozelin Protocol (SAP)</td> <td>gs y nection request and t then clock Edit I pour FADIUS cli Athibutes: Name Framed Protoc Service-Type</td> <td>DK Cancel Apply DK Cancel Apply Limixi Limixi Limixi Limixi Limixi Add standard RADIUS Attribute Add standard RADIUS Attribute To add an attribute to the settings, select the attribute, and then slick Add. To add a custom or predefined Vender Specific Attribute, and then slick Add. To add a custom or predefined Vender Specific Attribute, and then slick Add. To add a custom or predefined Vender Specific Attribute, and then slick Add. To add a custom or predefined Vender Specific Attribute, and then slick Add. To add a custom or predefined Vender Specific Attribute, and then slick Add. Add Attribute Information Attribute runnee: Attribute runnee: Attribute runnee: Attribute format: Attribute format:</td>	Server Test Properties Overview Conditions Constraints Settin Configue the settings for this network polic It conditions and constraints match the con- Settings: RADIUS Attributes Settings RADIUS Attributes Standard Vendor Specific Network Access Protection NAP Enforcement Setting and Remote Access Multink and Bandwidth Mozelin Protocol (SAP)	gs y nection request and t then clock Edit I pour FADIUS cli Athibutes: Name Framed Protoc Service-Type	DK Cancel Apply DK Cancel Apply Limixi Limixi Limixi Limixi Limixi Add standard RADIUS Attribute Add standard RADIUS Attribute To add an attribute to the settings, select the attribute, and then slick Add. To add a custom or predefined Vender Specific Attribute, and then slick Add. To add a custom or predefined Vender Specific Attribute, and then slick Add. To add a custom or predefined Vender Specific Attribute, and then slick Add. To add a custom or predefined Vender Specific Attribute, and then slick Add. To add a custom or predefined Vender Specific Attribute, and then slick Add. Add Attribute Information Attribute runnee: Attribute runnee: Attribute runnee: Attribute format: Attribute format:		
	Server Lest Properties Overview Conditions Constraints Settin Contigues the settings for this network polic It conditions and constraints match the con Settings: RADIUS Attributes Standard Vendor Specific Network Access Protection Network Access Protection Network Access NAP Enforcement Setting and Remote Access Multilink and Remote Access Withink and Remote Access	gs y nection request and t then click Edit I peur PADIUS cli Athibutes: Name FramedPhotoc Service-Type	DK Cancel Apply Imit at Imit		
Interwork Police File Action Vi File Action Vi RADIUS CI RA	Server Test Properties Overview Conditions Constraints Settin Configue the settings for this network polic If conditions and constraints match the con Settings: FADIUS Attributes Setting: NAPEnforcement Setting and Remote Access More in Protocol (BAP) Pibles Encryption	gs ynection request and t Yo send addition Hen click Edit I your PADIUS cli Athibutes: Name Framed-Protoc Service-Type	DK Cancel Apply Imit x1 Imit x1 Imit x1		
Inetwork Police File Action Vi RADDus cl RADDus cl RADDus Conne File Action File A	Server Lest Properties Diverview Conditions Constraints Settin Configues the satisfysion this network polic It conditions and constraints match the con Settings: RADIUS Attributes Standard Vendor Specific Network Access Protection NAP Enforcement Extended State Douting and Remote Access Multink and Remote Access Mote Protocol (SAP) The Remote Access Multink and Remote Access Multink and Remote Access Mote Protocol (SAP) The Remote Access Multink and Remote Access	gs y nection request and t To send addition Prenicick Edit I peur PADIUS dit Athibutes: Name Framed-Protoc Service-Type	DK Cancel Apply Limit xit Add scents, rettings are applied Add scents, rettings, asled the attribute, and then click Add. To add a custom or preferiend Vencior Soverite attribute, close this dation and select Vencior Soverite, and then click Add. Add a custom or preferiend Vencior Soverite attribute, close this dation and select Vencior Soverite, and then click Add. Add a custom or preferiend Vencior Soverite attribute, close this dation and select Vencior Soverite, and then click Add. Add a custom or preferiend Vencior Soverite attribute, close this dation and select Vencior Soverite, and then click Add. Add a custom or preferiend Vencior Soverite attribute, close this dation and select Vencior Soverite, and then click Add. Add a custom or preferiend Vencior Soverite attribute, close this dation and select Vencior Soverite attribute format: Advibute format: Advibute format: Closes Ensert the attribute value in: Fibered Gipte Take Fimered/Apple Take <td <="" colspan="2" td=""></td>		
Inetwork Police File Actor Vi File Actor Vi Restance RADIUS CI RADIUS CI RADIUS CI Renet Policies Policies Retwork A	Vertices Conditions Constraints Setting Divervices Conditions Constraints Setting Conditions end constraints match the constraints match the constraints match the constraints match the constraints Settings: PADIUS Attributes Standard Standard Standard Mathematical State NAP Enforcement Setting and Remote Access Multink and Bandwith Alocation Protocol (BAP) IP Filters Encorption IP Settings IP Settings	gs y nection request and t then click Edit. 1 your PADIUS cli Athibutes: Name Framed Protoc Service-Type Add	DK Cancel Apply Image: Second		
Inetwork Police File Action Vi RaDial Classification of the second seco	V Server Lest Properties Diverview Conditions Constraints Settin Corligue the satings for this network polic In conditions and constraints match the constraints match the constraints match the constraints match the constraints Settings: RADIUS Attributes Image: Standard Image: Nature Standard Image: Nature Standard Image:	ss) y nection request and t Pren click Edit I peur RADIUS cli Athibutes: Name Framed-Protoc Service-Type Add	DK Cancel Apply Image: Second		
Inetwork Pole File Actor Vi File Actor Vi Restance RADIUS CI RADIUS CI Renet Policies Policies Retwork A	Vertice: Conditions Constraints Setting Diverview Conditions Constraints Setting Conditions end constraints match the constraints Settings: FADIUS Attributes Standard Settings: Name of Specific Network Access Protection Name of Specific Network Access Protection Name of Specific Method State Routing and Remote Access Multilink and Bandwith afford Specific Multilink and Bandwith afford Specific Posting and Remote Access Multilink and Bandwith afford Specific IP Filters Encorpoint Posting and Remote Access Posting IP Filters Encorpoint IP Settings IP Settings	gs y nection request and b then cluk Edit. I yeur PADIUS cli Athibutes: Name Framed-Protoc Service-Type Add	DK Cancel Apply Image: Second		
Interwork Police File Action View View RADIUS RADIUS RADIUS Remat Policies Remat Network Conne Network Recounting Remat Templetes	V Server Lest Properties Diverview Conditions Constraints Settin Corligue the satings for this network polic In conditions and constraints match the constraints match the constraints match the constraints match the constraints Settings: RADIUS Attributes Image: Standsrd Image: Nature Access Protection Image: NAP Enforcement Image: Extended State Image: Multink and Bandwidth Alocation Protocol (BAP) Image: Ensystem Image: Ensystem Image: Ensystem Image: IP Settings	gs y nection request and t then click Edit I your PADIUS cli Attributes: Name FramedPhotoc Service-Type Add	DK Cancel Apply Image: Second Sec		
Inetwork Pole File Actor Vi File Actor Vi Restance RADIUS CI RADIUS CI RADIUS CI Restance	Server Lest Properties Dverview Conditions Constraints Settin Conditions end constraints match the constraints and constraints match the constraints matched state Mathematic Resource Access Multilink and Bandwidth allocation Protocol (BAP) IP Filters Encorption IP Settings	gs y nection request and b then cluk. Edit. 1 yeur PADIUS cli Athibutes: Name Framed-Protoc Service-Type Add	DK Cancel Apply Imit xil Imit xil He policy grants access, settings are appled. Add Standard RADIUS Attribute To add an attribute to the sattings, saled the attribute, and then click Add. To add a custom or precision Vendra Specific Attribute close this finion and select Vendra Specific, and then click Add. To add a custom or precisional Vendra Specific Attribute close this finion and select Vendra Specific, and then click Add. Add attribute to the sattings, saled the attribute close this finion and select Vendra Specific, and then click Add. Add Access type: Attribute number: Z5 Name Abstitute format: Callack/Number Callack/Number Class Formed AppleTake		
Inetwork Police File Action Vi WPS (Local) RADUS Climate Policies RADUS Conne Policies Policies Retwork A Retwork A<	VServer Lest Properties Diverview Conditions Constraints Settin Cortigues the satings for this network polic In conditions and constraints match the cort Settings: FADDUS Attributes Image: Standard Image: Name Environment Image: NAP Environment Image: Extended State Douting and Remote Access Multink and Bandwidth Alocation Protocol (BAP) IP Filess Image: Encryption Image: IP Settings	ss y nection request and the Prenclex Edit I peur RADIUS cli Athibutes: Name FramedPhotoc Service-Type Add	DK Cancel Apply DK Cancel Apply Imit x Imit x Imit x Imit x Imit x Add standard RADIUS Attribute X To add a custom or proteined Vencion Strengton, and then dick Add To add a custom or proteined Vencion Strengton, and then dick Add To add a custom or proteined Vencion Strengton Attribute Information Attribute number: Attribute number: Attribute format: OctedString Enter the attribute value in: Fixed d Formed AppleTake Format Annubre Catabastive Catab		

Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

Nota: Consulte Información Importante sobre Comandos de Debug antes de usar un comando debug.

Depuraciones de ASA

Habilite debug radius all en el ASA.

ciscoasa# test aaa-server authentication NPS host 10.105.130.51 username vpnuser password INFO: Attempting Authentication test to IP address <10.105.130.51> (timeout: 12 seconds) radius mkreq: 0x80000001 alloc_rip 0x787a6424 new request 0x80000001 --> 8 (0x787a6424) got user 'vpnuser' got password add_req 0x787a6424 session 0x80000001 id 8 RADIUS_REQUEST radius.c: rad_mkpkt RADIUS packet decode (authentication request) _____ Raw packet data (length = 65)..... |A.....~m.... 01 08 00 41 c4 1b ab 1a e3 7e 6d 12 da 87 6f 7f 40 50 a8 36 01 09 76 70 6e 75 73 65 72 02 12 28 @P.6..vpnuser..(c3 68 fb 88 ad 1d f2 c3 b9 9a a9 5a fa 6f 43 04 | .h.....Z.oC. 06 0a 69 82 de 05 06 00 00 00 00 3d 06 00 00 00 ..i...=.... 05 | . Parsed packet data..... Radius: Code = 1 (0x01)Radius: Identifier = 8 (0x08)Radius: Length = 65 (0x0041)Radius: Vector: C41BAB1AE37E6D12DA876F7F4050A836 Radius: Type = 1 (0x01) User-Name Radius: Length = 9 (0x09)Radius: Value (String) = 76 70 6e 75 73 65 72 vpnuser Radius: Type = 2 (0x02) User-Password Radius: Length = 18 (0x12)Radius: Value (String) = Radius: Type = 4 (0x04) NAS-IP-Address Radius: Length = 6 (0x06)Radius: Value (IP Address) = 10.105.130.52 (0x0A6982DE) Radius: Type = 5 (0x05) NAS-Port Radius: Length = 6 (0x06)Radius: Value (Hex) = 0x0Radius: Type = 61 (0x3D) NAS-Port-Type Radius: Length = 6 (0x06)Radius: Value (Hex) = 0x5send pkt 10.105.130.51/1645 rip 0x787a6424 state 7 id 8 rad_vrfy() : response message verified rip 0x787a6424 : chall_state '' : state 0x7 : regauth: c4 1b ab 1a e3 7e 6d 12 da 87 6f 7f 40 50 a8 36 : info 0x787a655c session_id 0x8000001 request_id 0x8 user 'vpnuser' response '***' app 0

reason 0 skey 'cisco' sip 10.105.130.51 type 1

RADIUS packet decode (response)

```
_____
Raw packet data (length = 78)....
02 08 00 4e e8 88 4b 76 20 b6 aa d3 0d 2b 94 37 | ...N..Kv ....+.7
bf 9a 6c 4c 07 06 00 00 00 01 06 06 00 00 02
                                              | ..lL.......
19 2e 9a 08 07 ad 00 00 01 37 00 01 02 00 0a 6a
                                              | ....i
2c bf 00 00 00 00 3c 84 0f 6e f5 95 d3 40 01 cf
                                              ,....<..n...@..
1e 3a 18 6f 05 81 00 00 00 00 00 00 00 03
                                             .:.0........
Parsed packet data....
Radius: Code = 2(0x02)
Radius: Identifier = 8 (0x08)
Radius: Length = 78 (0x004E)
Radius: Vector: E8884B7620B6AAD30D2B9437BF9A6C4C
Radius: Type = 7 (0x07) Framed-Protocol
Radius: Length = 6 (0x06)
Radius: Value (Hex) = 0x1
Radius: Type = 6 (0x06) Service-Type
Radius: Length = 6 (0x06)
Radius: Value (Hex) = 0x2
Radius: Type = 25 (0x19) Class
Radius: Length = 46 (0x2E)
Radius: Value (String) =
9a 08 07 ad 00 00 01 37 00 01 02 00 0a 6a 2c bf | ......j,.
00 00 00 00 3c 84 0f 6e f5 95 d3 40 01 cf 1e 3a
                                              18 6f 05 81 00 00 00 00 00 00 00 03
                                               .0.....
rad_procpkt: ACCEPT
RADIUS ACCESS ACCEPT: normal termination
RADIUS_DELETE
remove_req 0x787a6424 session 0x80000001 id 8
free_rip 0x787a6424
radius: send queue empty
INFO: Authentication Successful
```

Troubleshoot

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

- Asegúrese de que la conectividad entre el ASA y el servidor NPS sea buena. Aplique capturas de paquetes para asegurarse de que la solicitud de autenticación abandone la interfaz ASA (desde donde se puede acceder al servidor). Confirme que los dispositivos en la trayectoria no bloqueen el puerto UDP 1645 (puerto de autenticación RADIUS predeterminado) para asegurarse de que llegue al servidor NPS. Se puede encontrar más información sobre las capturas de paquetes en el ASA en <u>ASA/PIX/FWSM: Ejemplo de Captura de Paquetes con</u> <u>CLI y Configuración de ASDM</u>.
- Si la autenticación aún falla, mire en el visor de eventos en el NPS de Windows. En Visor de eventos > Registros de Windows, elija Seguridad. Busque eventos asociados con NPS alrededor del momento de la solicitud de autenticación.

Event Viewer						_ 5 ×	
nie action view nep							
Event Viewer (Local)	Security Number of events: 93 (1) New events available					Actions	
Windows Loos	Keywords	Date and Time	Source	Event 1D	Task Category	Security 🔺	
Application Setup System Forwardel Events Subscriptions Subscriptions	Audit Success Audit Success	2/10/2014 1:37:43 PM 2/10/2014 1:37:43 PM 2/10/2014 1:37:43 PM 2/10/2014 1:37:26 PM 2/10/2014 1:37:26 PM 2/10/2014 1:37:26 PM 2/10/2014 1:37:26 PM 2/10/2014 1:37:26 PM 2/10/2014 1:37:26 PM 2/10/2014 1:37:24 PM 2/10/2014 1:37:21 PM 2/10/2014 1:36:43 PM 2/10/2014 1:36:43 PM 2/10/2014 1:36:43 PM 2/10/2014 1:36:43 PM	Microso Microso Microso Microso Microso Microso Microso Microso Microso Microso Microso Microso Microso Microso	4634 4624 4672 6270 6270 4634 4624 4624 4624 4672 4634 4672 4634 4672 6273 4624	Logoff Logon Special Logon Network Policy Server Network Policy Server Logoff Logon Logon Credential Validation Logoff Logon Special Logon Special Logon Special Logon Logoff Logon Special Logon Logoff Logon Special Logon Logoff Logon Special Logon Logoff Logon Logoff Logon Logoff Logon Special Logon Logoff Logon Special Logon Logoff Logon Special Logon Logoff Logo Logo Logo Logoff Logo Logo	Create Custom View Create Custom View Import Custom View Clear Log Properties Properties Find Seve All Events As Attach a Task To this Log View Refresh Help Help	
	Audit Success	2/10/2014 1:35:47 PM	Microso	4672	 Agtach Task To This Event 	Event 6271 Microsoft Win.	
	Audit Success	2/10/2014 1:35:47 PM 2/10/2014 1:35:47 PM	Microso	4648 4769	K Save Selected Events	Event Properties	
	Event 6273, Microsof	t Windows security auditing.			Refresh	Attach Task To This Even	
	General Details				Heb	Copy Save Selected Events	

Una vez abiertas las propiedades del evento, debe poder ver el motivo del error, como se muestra en el ejemplo. En este ejemplo, PAP no se eligió como el tipo de autenticación en la política de red. Por lo tanto, la solicitud de autenticación falla.

```
Log Name: Security
Source:
            Microsoft-Windows-Security-Auditing
            2/10/2014 1:35:47 PM
Date:
Event ID: 6273
Task Category: Network Policy Server
Level: Information
Keywords:
           Audit Failure
            N/A
User:
Computer: win2k8.skp.com
Description:
Network Policy Server denied access to a user.
Contact the Network Policy Server administrator for more information.
User:
  Security ID:
                       SKP\vpnuser
  Account Name:
                        vpnuser
                         SKP
  Account Domain:
  Fully Qualified Account Name: skp.com/Users/vpnuser
Client Machine:
  Security ID:
                       NULL SID
  Account Name:
                        _
  Fully Qualified Account Name:
  OS-Version:
                       _
  Called Station Identifier:
  Calling Station Identifier:
NAS:
  NAS IPv4 Address:
                        10.105.130.69
  NAS IPv6 Address:
                         _
  NAS Identifier:
  NAS Port-Type:
                        Virtual
                    0
  NAS Port:
RADIUS Client:
  Client Friendly Name:
                           vpn
  Client IP Address:
                             10.105.130.69
```

Authentication Details: Connection Request Policy Name: vpn Network Policy Name: vpn Authentication Provider: Windows Authentication Server: win2k8.skp.com Authentication Type: PAP EAP Type: -Account Session Identifier: -Logging Results: Accounting information was written to the local log file. Reason Code: 66 Reason: The user attempted to use an authentication method that is not enabled on the matching network policy.