ليكو تانايب ةدعاق ةمدخ ليغشت ةداعإ متي ال فقوت دعب Cisco نم FirePOWER مدختسم

المحتويات

<u>المقدمة</u> الأعراض <u>الحل</u> المراجع

المقدمة

يمكن لعامل مستخدم Cisco مراقبة خادم Microsoft Active Directory (AD) والإبلاغ عن أنشطة تسجيل الدخول وتسجيل الخروج التي تم مصادقتها بواسطة خادم LDAP. يقوم مركز إدارة Firepower (FMC) بدمج هذه الأنشطة مع أحداث الأمان التي يجمعها من جهاز مدار FirePOWER. يوفر هذا المستند حلا لمشكلة عندما لا يبدأ "عامل المستخدم" عمله بعد أن تقوم بإيقاف خدمته.

الأعراض

يمكنك إستخدام الحل الموجود على هذا المستند إذا لاحظت الأعراض التالية مع خدمة وكيل المستخدم:

- تظهر واجهة عامل المستخدم الخدمة على أنها ليست قيد التشغيل.
- تظهر وحدة تحكم خدمة Windows، services.msc، حالة "وكيل مستخدم Cisco" على أنها فارغة، ويفشل في بدء الخدمة.
 - يظهر سجل أحداث Windows خطأ مماثلا ل "فشل علاقة الثقة بين المجال الأساسي والمجال الموثوق به"
 - يتم إنشاء ملف UserEncryptionBytes.bin على C:\ مع حجم صفر بايت.
- يظهر وضع تصحيح الأخطاء لعميل وكيل المستخدم رسائل الخطأ التالية في علامة التبويب "سجل" الخاصة بعميل المستخدم:

الحل

الخطوة 1: قم بتشغيل Microsoft Windows Services Console، services.msc. وهو يسمح لك بتعطيل خدمة Windows أو تمكينها.



الخطوة 2: انقر بزر الماوس الأيمن على خدمة وكيل المستخدم من Cisco وحدد **إيقاف** لإيقاف الخدمة.

Services

File Action View Help

_	×

	🛯 📑 📄 🖬 🕨 🖬 💵 📭					
Services (Local)	Services (Local)					
	Cisco Firepower User Agent for	Name	Description	Status	Startup Type	Log ^
	Active Directory	🎑 AppX Deployment Service (Provides inf	Running	Manual	Loc
	Stop the service	🌼 Arellia Agent	Arellia Man	Running	Automatic	Loc
	Restart the service	🎑 Auto Time Zone Updater	Automatica		Disabled	Loc
		Background Intelligent Tran	. Transfers fil	Running	Automatic (D	Loc
	Description:	Background Tasks Infrastru	Windows in	Running	Automatic	Loc
	Polls network logon information	Base Filtering Engine	The Base Fil	Running	Automatic	Loc
	from Active Directory servers and	BitDefender Threat Scanner	scan		Manual	Loc
	to Firepower Management Centers	BitLocker Drive Encryption	BDESVC hos		Manual (Trig	Loc
		Block Level Backup Engine	The WBENG		Manual (Tria	Loc
		Bluetooth Handsfree Service	The Plustee		Manual (Trig	Loc
		BranchCache	This service		Manual Manual	Net
		Certificate Propagation	Copies user	Running	Manual	Loc
		Cisco AnvConnect Secure	Cisco AnvC	Running	Automatic	Loc
		Cisco Firepower U		Running	Automatic	Loc
		Cisco Media Servic	L	Running	Automatic	Loc
		Cisco MSI Manage	0	Running	Automatic	Loc
		Client License Serv Pau	se		Manual (Trig	Loc
		CNG Key Isolation Res	ume	Running	Manual (Trig	Loc
		Code42 CrashPlan Res	tart	Running	Automatic	Loc
		COM+ Event Syste	Tasks >	Running	Automatic	Loc Y
	Educated (Structure)	<				>
		Ref	resh			
Stop service Cisco Firep	oower User Agent for Active Directory or	Pro	perties			
		Hel	p	1		

الخطوة 3: انتقل إلى C: محرك الأقراص.

🏪 🕑 📙 🖛	Drive Tools OSDisk (C:)			- 0
File Home Share V	/iew Manage			
\leftrightarrow \rightarrow \checkmark \Uparrow \clubsuit > This PC	> OSDisk (C:) >		v	Search OSDisk (C:)
🗸 🖈 Quick access 🔷 Nar	me	Date modified	Туре	Size
Desktop 🖈 🔤	ggsgsccmclient	7/19/2016 1:07 PM	File folder	
🗄 Documents 🖈 📃	IT_Logs	4/4/2017 8:58 AM	File folder	
📕 Downloads 🖈	Oracle	4/4/2017 8:57 AM	File folder	
Pictures	PerfLogs	10/30/2015 3:24 AM	File folder	
Desiter a	Program Files	4/4/2017 9:22 AM	File folder	
Desktop	Program Files (x86)	4/4/2017 9:20 AM	File folder	
J Music	Users	7/18/2016 2:04 PM	File folder	
Temp	Windows	4/4/2017 10:04 AM	File folder	
📑 Videos 👫	CiscoUserAgent	4/4/2017 10:27 AM	SQL Server Compact Edition Database File	212 KB
This PC	msdia80.dll	9/22/2005 8:39 PM	Application extension	874 KB
	triggerfullhinv	7/18/2016 7:02 PM	Text Document	1 KB
> Desktop	UserAgentEncryptionBytes.bin	4/4/2017 10:16 AM	BIN File	1 KB
> 🖆 Documents				
> 🕂 Downloads				
> 🎝 Music				
> 📰 Pictures				
> 🗧 Videos				
> 🏪 OSDisk (C:)				
> 🛖 Shared Folders (
> 💣 Network 🗸 🗸				

الخطوة 4: احذف ملف UserAgentEncryptionBytes.bin.

File Home	Share	View						~ 🤇
← → • ↑ ⊑	> This	PC > OS	Disk (C:) >			ٽ ~	Search OSDisk (C:)	<i>م</i>
🖈 Quick access	^	Name	~	Date modified	Туре	Size		
Desktop	*	📙 ggsgs	sccmclient	7/19/2016 1:07 PM	File folder			
Documents	*	IT_Lo	gs	4/4/2017 8:58 AM	File folder			
	<u></u>	Oracl	e	4/4/2017 8:57 AM	File folder			
Dictures	^	PerfLo	ogs	10/30/2015 3:24 AM	File folder			
Pictures	*	- Progr	ram Files	4/4/2017 9:22 AM	File folder			
Desktop		Progr	ram Files (x86)	4/4/2017 9:20 AM	File folder			
Music		Users	(7/18/2016 2:04 PM	File folder			
Temp		Wind	ows	4/4/2017 10:04 AM	File folder			
📑 Videos		💾 Cisco	UserAgent	4/4/2017 10:28 AM	SQL Server Compact Edition Database File		212 KB	
This DC		🗟 msdia	a80.dll	9/22/2005 8:39 PM	Application extension		874 KB	
This PC		📄 trigge	erfullhinv	7/18/2016 7:02 PM	Text Document		1 KB	
Desktop		User	agentEncountionPuter him	4/4/2017 10:16 AM	BIN File		1 KB	
Documents			Open with					
👆 Downloads			Scan with Windows Defender					
👌 Music			💟 Scan for threats					
Pictures			Sourcefire	>				
📑 Videos			Restore previous versions					
🏪 OSDisk (C:)			Send to	>				
🛖 Shared Folde	rs (°		Cut					
🔿 Network	~		Conv					
12 items 1 item s	elected 2	24 bytes	Сору					
			Create shortcut					
			😌 Delete					
			💎 Rename					
			Properties					

الخطوة 5: احذف ملف Cisco UserAgent، وهو ملف قاعدة بيانات SQL Server Compact Edition.

Lange Home Share) View							- 0
\leftarrow \rightarrow \checkmark \Uparrow \blacksquare \rightarrow This	s PC → OSD	isk (C:) →				~	Ō	Search OSDisk (C:)
A Quick access	Name	^	Date m	odified	Туре		Size	
Desktop 🖈	ggsgs	comolient	7/19/20	16 1:07 PM	File folder			
😫 Documents 🖈	📙 IT_Log	IS	4/4/201	7 8:58 AM	File folder			
Downloads *	Oracle		4/4/201	7 8:57 AM	File folder			
Pictures *	PerfLo	gs	10/30/2	015 3:24 AM	File folder			
Desisten	Progra	im Files	4/4/201	7 9:22 AM	File folder			
Desktop	Progra	ım Files (x86)	4/4/201	7 9:20 AM	File folder			
J Music	Users		7/18/20	16 2:04 PM	File folder			
- Temp	- Windo	WS .	4/4/201	7 10:04 AM	File folder			
Videos	Ciscol	JserAgent	4/4/201	7 10:28 AM	SQL Server Compact Edition Database File			212 KB
This PC	<u>s</u>	Scan with Windows Defender		05 8:39 PM	Application extension			874 KB
Deskton	■ t	Open with		16 7:02 PM	Text Document			1 KB
Documents	U	Scan for threats						
Downloads		Sourcefire	>					
Music		Restore previous versions						
Pictures		Send to	>					
🚆 Videos		Cut						
SDisk (C:)		Сору						
🛖 Shared Folders (Create shortcut						
💣 Network 🗸 🗸	٩	Delete						
11 items 1 item selected 2	212 КВ 🎈	Rename						
		Properties		E ANTERN				

الخطوة 6: ارجع إلى services.msc. انقر بزر الماوس الأيمن على خدمة وكيل المستخدم من Cisco، وحدد **خصائص**، ثم حدد علامة التبويب **تسجيل الدخول**، وقم بتكوين مستخدم كتسجيل دخول مستخدم AD. طقطقة **يطبق** عندما يتم.

🔅 Services					- 🗆	\times
File Action View H	lelp					
File Action View H Services (Local)	Cisco Firepower User Age General Log On Recor Log on as: O Local System account Allow service to int O This account: Password: Confirm password:	ent for Active Directory Properties (Local very Dependencies t teract with desktop test Browse	C × cription litates rides su cesses rides in lia Man omatic sfers fi dows i Base F	n Status t Running u in Running if n Running a il Running il Running il	Startup Type Manual (Trig Manual Manual Manual Automatic Disabled Automatic (D Automatic Automatic Manual	× Log ^ Loc Loc Loc Loc Loc Loc Loc Loc
E	xtended / Standard /	OK Cancel A	SVC he WBEN bles wi Blueto servic ies use o Anyt s netw bles Ci bles Ci bles Ci	os G e er Running C Running o Running s Running s Running	Manual (Trig Manual (Trig Manual (Trig Manual (Trig Manual Manual Automatic Automatic Automatic Automatic Manual (Trig	Loc Loc Loc Loc Loc Loc Loc Loc Loc Loc

الخطوة 7: في Services.msc، انقر فوق **بدء** ل **Cisco Firepower User Agent** لخدمة Active Directory.

Services					- 🗆	×
File Action View	Help					
🔶 🔿 📘 🗖 🖸	à 🗟 🛛 📷 🕨 🔳 II IV					
🔍 Services (Local)	🔍 Services (Local)					
	Cisco Firepower User Agent for	Name	Description	Status	Startup Type	Log ^
	Active Directory	Application Information	Facilitates t	Running	Manual (Trig	Loc
	Start the service	🎑 Application Layer Gateway	Provides su		Manual	Loc
	State the service	🏟 Application Management	Processes in	Running	Manual	Loc
		🎑 AppX Deployment Service (Provides inf		Manual	Loc
	Description:	🔍 Arellia Agent	Arellia Man	Running	Automatic	Loc
	from Active Directory servers and	🔍 Auto Time Zone Updater	Automatica		Disabled	Loc
	reports user to IP address mappings	Background Intelligent Tran	Transfers fil	Running	Automatic (D	Loc
	to Firepower Management Centers	Background Tasks Infrastru	Windows in	Running	Automatic	Loc
		Base Filtering Engine	The Base Fil	Running	Automatic	Loc
		BitDefender Threat Scanner	scan		Manual	Loc
		BitLocker Drive Encryption	BDESVC hos		Manual (Trig	Loc
		Block Level Backup Engine	The WBENG		Manual	Loc
		Bluetooth Handsfree Service	Enables wir		Manual (Trig	Loc
		Bluetooth Support Service	The Bluetoo		Manual (Trig	Loc
		BranchCache	This service		Manual	Net
		Certificate Propagation	Copies user	Running	Manual	Loc
		Cisco AnyConnect Secure	Cisco AnyC	Running	Automatic	Loc
		Cisco Firepower User Agent	Polls netwo		Automatic	Loc
		Cisco Media Services Interfa	Enables Cis	Running	Automatic	Loc
		Cisco MSI Management Ser	Enables Cis	Running	Automatic	Loc
		Client License Service (ClipS	Provides inf		Manual (Trig	Loc V
	Extended Standard /					-

الخطوة 8: تحقق من حجم ملف UserAgentEncryptionBytes.bin. يجب ألا تكون 0 كيلوبايت.

→ * ↑ → Thi	is PC > OSDisk (C:)			5 V	Search OSDisk (C:))
Quick access	Name	Date modified	Туре	Size		
Desktop 🖈	ggsgsccmclient	7/19/2016 1:07 PM	File folder			
Documents 🖈	IT_Logs	4/4/2017 8:58 AM	File folder			
Downloads 🖈	Oracle	4/4/2017 8:57 AM	File folder			
Dictures	PerfLogs	10/30/2015 3:24 AM	File folder			
		4/4/2017 9:22 AM	File folder			
Desktop	Program Files (x86)	4/4/2017 9:20 AM	File folder			
Music	Users	7/18/2016 2:04 PM	File folder			
Temp	Windows	4/4/2017 10:04 AM	File folder			
Videos	🛅 CiscoUserAgent	4/4/2017 10:36 AM	SQL Server Compact Edition Database File	21	12 KB	
This DC	Smsdia80.dll	9/22/2005 8:39 PM	Application extension	87	74 KB	
This PC	triggerfullhinv	7/18/2016 7:02 PM	Text Document		1 KB	
Desktop	UserAgentEncryptionBytes.bin	4/4/2017 10:35 AM	BIN File		1 KB	
Documents						
 Downloads 						
Music						
Pictures						
Videos						
OSDisk (C:)						
Shared Folders (\\vr						
Sildica i olacis (((ii						

الخطوة 9: إضافة وحدات التحكم في المجال ومركز إدارة FirePOWER إلى عميل وكيل المستخدم. الرجاء التأكد من إضافة وحدات التحكم بالمجال/المضيف المحلي قبل إضافة مركز إدارة Firepower إلى "عميل المستخدم".

Active Directory Servers					
Host	Polling Status	Last Polled	Real-time Status	Last Real-time Report	Real-time
Active Directory Server Pr	Server Name/IP Address: Domain: Authorized User: Password:	domain		Add	Remove

المراجع

- <u>دليل تكوين وكيل مستخدم Firepower، الإصدار 2.3</u>
- يتوقف عميل المستخدم عن الخروج عن المسار إذا تعذر عليه ترجمة حساب الخدمة إلى معرف الأمان (CSCuw20184)
- منح الحد الأدنى من الإذن لحساب مستخدم Active Directory المستخدم بواسطة عامل مستخدم Sourcefire

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