Cisco Firepower使用者代理資料庫服務在停止後 不重新啟動

目錄

<u>簡介</u> <u>症狀</u> <u>解決方案</u> <u>參考資料</u>

簡介

思科使用者代理可以監視Microsoft Active Directory(AD)伺服器並報告由LDAP伺服器進行身份驗證的登入和註銷活動。Firepower管理中心(FMC)將這些活動與 其從Firepower受管裝置收集的安全事件相整合。當您停止服務後,使用者代理不啟動時,本文檔便為問題提供了解決方案。

症狀

如果在使用者代理服務中發現以下症狀,則可以使用本文檔上的解決方案:

- 使用者代理介面將服務顯示為Not Running。
- •Windows服務控制檯services.msc將思科使用者代理狀態顯示為空白,並且無法啟動服務。
- Windows事件日誌顯示類似於「主域和受信任域之間的信任關係失敗」的錯誤
- 在C:∖上建立UserEncryptionBytes.bin 檔案,其大小為零。
- 使用者代理客戶端的調試模式在使用者代理的「日誌」頁籤中顯示以下錯誤消息:

,"debug","[0102] - An error occured while fetching encryption bytes from 'C:\UserAgentEncryptionBytes.bin':

The trust relationship between the primary domain and the trusted domain failed.. "

,"error","[0102] - An error occured while fetching encryption bytes from
'C:\UserAgentEncryptionBytes.bin':
Specified key is not a valid size for this algorithm.."

,"error","[0002] - Error connecting to 10.85.3.122: System.UnauthorizedAccessException: Access is denied. (Exception from HRESULT: 0x80070005 (E_ACCESSDENIED)) 解決方案

第1步:運行Microsoft Windows服務控制檯services.msc。它允許您禁用或啟用Windows服務。



第2步:按一下右鍵Cisco User Agent服務,然後選擇**Stop**停止該服務。

🔍 Services

File Action View Help

- 🗆 X	-		\times
-------	---	--	----------

	à 🗟 🛛 📷 🕨 🗰 🕕 🕨					
🔍 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
		鵒 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
	reports user to IP address mappings	BitLocker Drive Encryption	BDESVC hos		Manual (Trig	Loc
	to Firepower Management Centers	Block Level Backup Engine	The WBENG		Manual	Loc
		Bluetooth Handsfree Service	Enables wir		Manual (Trig	Loc
		Bluetooth Support Service	The Bluetoo		Manual (Trig	Loc
		SranchCache	This service		Manual	Net
		Certificate Propagation	Copies user	Running	Manual	Loc
		Cisco AnyConnect Secure	Cisco AnyC	Running	Automatic	Loc
		Cisco Firepower Us Star	t	Running	Automatic	Loc
		Cisco Media Servic	•	Running	Automatic	Loc
		Cisco MSI Manage	ce.	Running	Automatic	Loc
		Client License Serv	172.0		Manual (Trig	Loc
		CNG Key Isolation		Running	Manual (Trig	LOC
		Code42 CrashPlan Rest	аπ	Running	Automatic	LOC
		< All T	asks >	Kunning	Automatic	>
	Extended Standard	Refr	esh			
Stop service Cisco Fired	oower User Agent for Active Directory or	n Local Computer	can			
		Pro	perties	-		
		Help	0	11		

步驟3:導航至C:驅動器。

1	🗸 📑 🗧		Drive Tools OSDisk (C:)						- 0
File	Home Sha	are View	Manage				_		
←	→ · T ► ·	This PC > 0	SDISK (C:) >			~	C	Search	OSDisk (C:)
× 🖈	Quick access	^ Name	^	Date modified	Туре		Size		
	Desktop 🖈	ggsg	gsccmclient	7/19/2016 1:07 PM	File folder				
4	Documents 🖈	IT_L	ogs	4/4/2017 8:58 AM	File folder				
_	Downloads 🖈	Orac	le	4/4/2017 8:57 AM	File folder				
	Distance	Perf	Logs	10/30/2015 3:24 AM	File folder				
-	Pictures 🖈	Prog	gram Files	4/4/2017 9:22 AM	File folder				
	Desktop	Prog	gram Files (x86)	4/4/2017 9:20 AM	File folder				
	Music	User	5	7/18/2016 2:04 PM	File folder				
	Temp	Win	dows	4/4/2017 10:04 AM	File folder				
	Videos	🗎 Cisc	oUserAgent	4/4/2017 10:27 AM	SQL Server Compact Edition Database File			212 KB	
	This DC	🗟 msd	ia80.dll	9/22/2005 8:39 PM	Application extension			874 KB	
* =	This PC	📄 trigg	gerfullhinv	7/18/2016 7:02 PM	Text Document			1 KB	
>	Desktop	🗋 User	AgentEncryptionBytes.bin	4/4/2017 10:16 AM	BIN File			1 KB	
>	Documents								
>	 Downloads 								
> 👌	Music								
>	Pictures								
>	Videos								
> =	OSDisk (C:)								
> =	Shared Folders (
> 🥔 12 ite	Network	~							

第4步:刪除此UserAgentEncryptionBytes.bin檔案。

File	Home	Share	View						~ (
← →	· 🛧 🐂	> This	PC > OS	Disk (C:) >			ٽ ~	Search OSDisk (C:)	Q
📌 Q	uick access	^	Name	^	Date modified	Туре	Size		
	Desktop 🧳	*	ggsgs	sccmclient	7/19/2016 1:07 PM	File folder			
a	Documents		IT_Lo	gs	4/4/2017 8:58 AM	File folder			
	Downloads		Oracl	e	4/4/2017 8:57 AM	File folder			
	Distance (PerfL	ogs	10/30/2015 3:24 AM	File folder			
	Pictures)	*	Progr	am Files	4/4/2017 9:22 AM	File folder			
	Desktop		Progr	am Files (x86)	4/4/2017 9:20 AM	File folder			
ا ا	Music		Users		7/18/2016 2:04 PM	File folder			
	Temp		- Wind	ows	4/4/2017 10:04 AM	File folder			
	/ideos		📸 Cisco	UserAgent	4/4/2017 10:28 AM	SQL Server Compact Edition Database File		212 KB	
Т	in DC		🗟 msdia	a80.dll	9/22/2005 8:39 PM	Application extension		874 KB	
	IIS PC		📄 trigge	erfullhinv	7/18/2016 7:02 PM	Text Document		1 KB	
	Desktop		User/	ContEncontionPutor bin	4/4/2017 10:16 AM	BIN File		1 KB	
	Documents			Open with					
- 🕂 I	Downloads			Scan with Windows Defender					
🌙 👌 I	Music			Scan for threats					
	Pictures			Sourcefire	>				
	/ideos			Restore previous versions					
<u> </u>	OSDisk (C:)			Send to	<u> </u>				
= :	Shared Folders	s C							
- N	ab			Cut					
12 itom	etwork	v lected 2	Abstac	Сору					8 6
12 item	s intenisei	lected 2	- bytes	Create shortcut					
				😌 Delete		and the second s			
				💡 Rename					
				Properties					

第5步:刪除CiscoUserAgent檔案,該檔案是SQL Server Compact Edition資料庫檔案。

🟪 💆 📑 🖛 OSDisk (C:)						- 0
File Home Share \leftarrow \rightarrow \uparrow \blacksquare \rightarrow	View PC > OSDisk (C:) >			~	Ū	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			
L Downloads		4/4/2017 8:57 AM	File folder			
	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			
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 10:28 AM	SQL Server Compact Edition Database File		2	12 KB
This PC	Scan with Windows Defender	05 8:39 PM	Application extension		8	74 KB
Deckton	t Open with	16 7:02 PM	Text Document			1 KB
Documents	Scan for threats					
Downloads	Sourcefire	>				
b Music	Restore previous versions					
Pictures	Send to	>				
Videos	Cut					
SDisk (C:)	Сору					
🛖 Shared Folders (Create shortcut					
🔿 Network 🗸 🗸	💎 Delete					
11 items 1 item selected 2	12 KB 💔 Rename					
	Properties	Edda and	I MARINA CONTRACTOR			

第6步:返回services.msc。按一下右鍵Cisco User Agent服務,選擇**Properties**,然後選擇**Log On**頁籤,將使用者配置為AD使用者登入。完成後按一下**Apply**。

Services						- 🗆	\times
File Action View	Help						
File Action View	Help Cisco Firepower User Ag General Log On Reco Log on as: O Local System accour Allow service to in O This account: Password: Confirm password:	ent for Active Directory P very Dependencies It teract with desktop test	Properties (Local C >	cription litates t /ides su cesses in /ides inf lia Man pmatica sfers fil dows in	Status Running Running Running Running Running	Startup Type Manual (Trig Manual Manual Manual Automatic Disabled Automatic (D Automatic	Log ^ Loc Loc Loc Loc Loc Loc Loc Loc
t	Evtended (Standard /	OK (Cancel Apply	Base Fil SVC hos WBENG bles wir Bluetoo service ies user o AnyC s netwo bles Cis ples Cis vides inf	Running Running Running Running Running Running	Automatic Manual Manual (Trig Manual (Trig Manual (Trig Manual Manual Automatic Automatic Automatic Automatic Manual (Trig	Loc Loc Loc Loc Loc Loc Loc Loc Loc Loc
	Extended Standard						

第7步:在services.msc上,按一下**Cisco Firepower User Agent** for Active Directory服務的**啟動**。

🍓 Services					- 🗆	×
File Action View	Help					
♦ ♦ 0) 📑 🛛 🖬 🕨 🖬 🗤					
🔍 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
		Application Management	Processes in	Running	Manual	Loc
		AppX Deployment Service (Provides inf		Manual	Loc
	Polls network logon information	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
		RIuetooth Support Service	The Bluetoo		Manual (Trig	Loc
		SranchCache	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 ⊻
		<				>
	Extended Standard					

第8步:驗證UserAgentEncryptionBytes.bin檔案的大小。不應為0 KB。

	s PC > OSDISK (C:)			∿ ©	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	2	12 KB	
This DC	msdia80.dll	9/22/2005 8:39 PM	Application extension	8	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 ())						

第9步:將域控制器和Firepower管理中心新增到使用者代理客戶端。請務必先新增域控制器/本地主 機,然後再將Firepower管理中心新增到使用者代理。

Active Directory Servers					
Host	Polling Status	Last Polled	Real-time Statu	us Last Real-time Report	Real-time
Active Directory Server Po Active Directory Server Ma	Server Name/IP Address: Domain: Authorized User: Password:	r Configur — domain		A	dd Remove
	Local Login IP Address:	<select></select>	~		

參考資料

- Firepower使用者代理配置指南2.3
- <u>如果使用者代理無法將服務帳戶轉換為安全識別符號(CSCuw20184),則停止離線</u>
- <u>向Sourcefire使用者代理使用的Active Directory使用者帳戶授予最低許可權</u>