停止后,Cisco Firepower用户代理数据库服务不 会重新启动

目录

<u>简介</u> <u>症状</u> <u>解决方案</u> <u>参考</u>

简介

思科用户代理可以监控Microsoft Active Directory(AD)服务器,并报告由LDAP服务器进行身份验证的登录和注销活动。Firepower管理中心(FMC)将这些活动与 从Firepower受管设备收集的安全事件相集成。本文档针对在停止用户代理服务后用户代理未启动的问题提供解决方案。

症状

如果您注意到用户代理服务出现以下症状,则可使用本文档中的解决方案:

- 用户代理界面将服务显示为"未运行"。
- •Windows服务控制台services.msc将Cisco用户代理状态显示为空白,并且无法启动服务。
- Windows事件日志显示类似于"主域和受信任域之间的信任关系失败"的错误
- 在C:\上创建一个文件UserEncryptionBytes.bin,其大小为零字节。
- 用户代理客户端的调试模式在用户代理的"日志"选项卡中显示以下错误消息:

,"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)) 解决方案

步骤 1:运行Microsoft Windows Services Console, services.msc。它允许您禁用或启用 Windows服务。



步骤 2:右键点击Cisco User Agent服务,然后选择**Stop**以停止服务。

🔍 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		

步骤3:导航至C:驱动器。

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	~							

步骤4:删除此UserAgentEncryptionBytes.bin文件。

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			
	Documents		IT_Lo	gs	4/4/2017 8:58 AM	File folder			
	Downloads		Oracl	e	4/4/2017 8:57 AM	File folder			
	Downloads ,		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			
<u>ا</u>	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	
— —	- 00		🗟 msdia	a80.dll	9/22/2005 8:39 PM	Application extension		874 KB	
-	nis PC		📄 trigge	erfullhinv	7/18/2016 7:02 PM	Text Document		1 KB	
	Desktop		User A	aontEncontionPutor hin	4/4/2017 10:16 AM	BIN File		1 KB	
	Documents			Open with					
-	Downloads			Scan with Windows Defender					
۵.	Music			💙 Scan for threats					
	Pictures			Sourcefire	>				
-	Videos			Restore previous versions					
-	OSDisk (C:)			Send to	>				
=	Shared Folders	s (°		Cut					
💣 N	etwork	~		Conv					
12 item	s 1 item se	lected 2	4 bytes						
				Create shortcut		Carl Courses of MIN marks			
				V Delete		I I I I I I I I I I I I I I I I I I I			
				V Rename		and all the states			
				Properties					

步骤 5: 删除CiscoUserAgent文件,该文件是SQL Server Compact Edition数据库文件。

Le Home Share	View							- 0
\leftarrow \rightarrow \checkmark \Uparrow \blacksquare \succ This	PC > OSDisk	(C:) >				~	Ö	Search OSDisk (C:)
A Quick access	Name	^	Date modified	I	Туре		Size	
Desktop 🖈	ggsgsccm	nclient	7/19/2016 1:07	7 PM	File folder			
🛱 Documents 🖈	IT_Logs		4/4/2017 8:58 A	AM	File folder			
L Downloads	Oracle		4/4/2017 8:57 A	AM	File folder			
Dictures	PerfLogs		10/30/2015 3:24	24 AM	File folder			
	Program F	Files	4/4/2017 9:22 A	AM	File folder			
Desktop	🔤 Program F	Files (x86)	4/4/2017 9:20 A	AM	File folder			
J Music	Users		7/18/2016 2:04	1 PM	File folder			
Temp	Windows		4/4/2017 10:04	1 AM	File folder			
📑 Videos	CiscoUser	Agent	4/4/2017 10:28	3 AM	SQL Server Compact Edition Database File			212 KB
This PC	🖄 i Sca	an with Windows Defender	05 8:39 1	PM	Application extension			874 KB
Desiten	t Op	oen with	16 7:02 1	2 PM	Text Document			1 KB
Desktop Documents	💟 Sca	an for threats						
Downloads	So:	urcefire	>					
b Music	Re	store previous versions						
Pictures	Ser	nd to	>					
Videos	Cu	ıt						
SDisk (C:)	Co	рру						
🛖 Shared Folders (Cre	eate shortcut						
💣 Network 🗸 🗸	🍤 De	lete						
11 items 1 item selected 2	212 KB 🎈 Rei	name						
	Pro	operties	E.A.H					

步骤 6:返回services.msc。右键单击Cisco User Agent服务,选择**Properties**,然后选择**Log On**选 项卡,并将用户配置为AD用户登录。完成后**单击"**应用"。

Services				- 🗆	\times
File Action View	Help				
← ➡ I III III II III III	Cisco Firepower User Agent for Active Directory Properties (Local C × General Log On Recovery Dependencies Log on as:	cription litates t	Status Running	Startup Type Manual (Trig	Log ^
S R D P fr r t c	Confirm password:	litates t /ides su cesses in /ides inf lia Man pmatica pmatica sfers fil dows in Base Fil N SVC hos WBENG ples wir Bluetoo service ies user	Running Running Running Running Running Running	Manual (Trig Manual Manual Automatic Disabled Automatic (D Automatic Manual Manual (Trig Manual Manual (Trig Manual Manual Manual Manual	Loc Loc Loc Loc Loc Loc Loc Loc Loc Loc
	OK Cancel Apply	o AnyC s netwo oles Cis oles Cis vides inf	Running Running Running Running	Automatic Automatic Automatic Automatic Manual (Trig	Loc Loc Loc Loc Loc ¥
\	Extended Standard /				

步骤 7:在services.msc上,单击**Start**以查看**Cisco Firepower User Agent for Active Directory**服务。

🍓 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 Manual Loc Manual Loc Manual Loc Running Automatic Loc Disabled Loc Running Automatic (D Loc Running Automatic Loc Running Automatic Loc Manual Loc Manual (Trig Loc Manual (Trig Loc Manual (Trig 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					

步骤 8::验证UserAgentEncryptionBytes.bin文件的大小。不应为0 KB。

🟪 🔽 📙 🖛 OSDisk (C:))			-	D X
File Home Share	View				~ 🕐
← → × ↑ 🏪 > This	PC > OSDisk (C:)			✓ ひ Search OSDisk (C:)	<i>م</i>
🖈 Quick access	Name	Date modified	Туре	Size	
Desktop 🖈	📙 ggsgsccmclient	7/19/2016 1:07 PM	File folder		
😫 Documents 🛷		4/4/2017 8:58 AM	File folder		
Downloads *		4/4/2017 8:57 AM	File folder		
Dictures #		10/30/2015 3:24 AM	File folder		
	📙 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 10:36 AM	SQL Server Compact Edition Database File	212 KB	
This DC	🗟 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 10:35 AM	BIN File	1 KB	
Documents					
👆 Downloads					
b Music					
Pictures					
Videos					
SDisk (C:)					
👳 Shared Folders (\\vr					
💣 Network					
12 items 1 item selected 2	24 bytes				

步骤 9:将域控制器和Firepower管理中心添加到用户代理客户端。请确保在将Firepower管理中心添加到用户代理之前添加域控制器/本地主机。

Active Directory Servers					
Host	Polling Status	Last Polled	Real-time Status	Last Real-time Report	Real-time
-3	* Active Directory Server	r Configur —			
	Server Name/IP Address:				
	Domain:	domain			
Active Directory Server Po	Authorized User:				
Active Directory Server Ma	Password:			Add	Remove
	Local Login IP Address:	<select></select>	~		

参考

- Firepower用户代理配置指南,2.3
- •<u>如果用户代理无法将服务帐户转换为SecurityIdentifier(CSCuw20184),则停止脱轨</u>
- <u>向Sourcefire用户代理使用的Active Directory用户帐户授予最低权限</u>