O serviço de banco de dados do agente de usuário do Cisco Firepower não é reiniciado após uma parada

Contents

Introduction Sintomas Solução Referências

Introduction

Um Agente de Usuário Cisco pode monitorar o servidor do Microsoft Ative Diretory (AD) e relata as atividades de login e logoff autenticadas por um servidor LDAP. O Firepower Management Center (FMC) integra essas atividades aos eventos de segurança que coleta de um dispositivo gerenciado Firepower. Este documento fornece uma solução para um problema quando o Agente de usuário não é iniciado depois que você interrompe o serviço.

Sintomas

Você pode usar a solução neste documento se notar os seguintes sintomas com seu serviço de Agente de Usuário:

- A interface do agente de usuário mostra o serviço como Não em execução.
- O Console de serviço do Windows, services.msc, mostra o status do Agente de usuário Cisco como em branco e falha ao iniciar o serviço.
- O log de eventos do Windows mostra um erro semelhante a "A relação de confiança entre o domínio primário e o domínio confiável falhou"
- Um arquivo UserEncryptionBytes.bin é criado em C:\ com tamanho zero byte.
- O modo de depuração de um cliente de agente de usuário mostra as seguintes mensagens de erro na guia Log (Log) do agente de usuário:

,"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)) Solução

Passo 1: Execute o Console do Microsoft Windows Services, services.msc. Permite desativar ou ativar um serviço do Windows.



Passo 2: Clique com o botão direito do mouse no serviço Cisco User Agent e selecione **Stop** para interromper o serviço.

🔍 Services

File Action View Help

_	×
	<i>'</i> `

	2 🗟 🛛 📷 🕨 🔲 II 🕪					
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
	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	2	Running	Automatic	Loc
		Cisco MSI Manage		Running	Automatic	Loc
		Client License Serv	se		Manual (Trig	Loc
		CNG Key Isolation Resi	ume	Running	Manual (Trig	Loc
		Code42 CrashPlan Rest	tart	Running	Automatic	Loc
		COM+ Event Syste	Tasks >	Running	Automatic	Loc Y
	Estanded (Standard (×				,
	Extended Standard	Refr	esh			
Stop service Cisco Firep	oower User Agent for Active Directory or	n Local Computer Pro	perties			
		Hel	p	11		

Passo 3: Navegue até o C: unidade.

🟪 🕑 📙 🚽	Drive Tools OSDisk (C:)				- 0
$\leftarrow \rightarrow \checkmark \land \stackrel{\text{Home}}{=} \rightarrow \text{This}$	PC > OSDisk (C:) >			C) Sear	ch OSDisk (C:)
	N ^	D	-		
🗸 🖈 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		
	Program Files	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	隌 CiscoUserAgent	4/4/2017 10:27 AM	SQL Server Compact Edition Database File	212 K	В
V This DC	Smooth Strategy Strat	9/22/2005 8:39 PM	Application extension	874 K	В
	triggerfullhinv	7/18/2016 7:02 PM	Text Document	1 K	В
> Desktop	UserAgentEncryptionBytes.bin	4/4/2017 10:16 AM	BIN File	1 K	В
> 🔮 Documents					
> 🕂 Downloads					
> 🁌 Music					
> 📰 Pictures					
> 📕 Videos					
> L OSDisk (C:)					
Shared Folders (
/ T shared Polders (
> 💣 Network 🗸 🗸					
12 items					

Passo 4: Exclua este arquivo UserAgentEncryptionBytes.bin.

File	Home	Share	View							~ 🤇
← →	· ↑ 🖢	> This	PC → OSE	Disk (C:) >			~	Q	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_Log	gs	4/4/2017 8:58 AM	File folder				
	Downloads		- Oracle	e	4/4/2017 8:57 AM	File folder				
	Distance		- PerfLo	ogs	10/30/2015 3:24 AM	File folder				
	Pictures	*	- Progra	am Files	4/4/2017 9:22 AM	File folder				
	Desktop		Progra	am Files (x86)	4/4/2017 9:20 AM	File folder				
1	Music		Users		7/18/2016 2:04 PM	File folder				
	Temp		- Winde	ows	4/4/2017 10:04 AM	File folder				
2	Videos		隌 Cisco	UserAgent	4/4/2017 10:28 AM	SQL Server Compact Edition Database File			212 KB	
Пт	his DC		🗟 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	contEncontionPutor 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	<u> </u>					
Ŧ	Shared Folders	s (°			<u> </u>					
🔿 N	letwork	~		Carv						
12 item	s 1 item sel	lected 2	4 bytes	сору						
				Create shortcut		Contract of MIN 1 - 1	100000			
				💛 Delete						
				🤤 Rename						
-				Properties						

Passo 5: Exclua o arquivo CiscoUserAgent, que é um arquivo de banco de dados do SQL Server Compact Edition.

\leftarrow \rightarrow \checkmark \uparrow 🖕 \flat This	PC > OSE	Disk (C:) >				~	ට Search	n OSDisk (C:)
A Quick access	Name	^	Date me	odified	Туре		Size	
Desktop 🖈	📙 ggsgs	ccmclient	7/19/20	16 1:07 PM	File folder			
	IT_Lo	gs	4/4/201	7 8:58 AM	File folder			
- Downloads	- Oracle	e	4/4/201	7 8:57 AM	File folder			
	- PerfLo	ogs	10/30/2	015 3:24 AM	File folder			
	Progr	am Files	4/4/201	7 9:22 AM	File folder			
Desktop	Progr	am Files (x86)	4/4/201	7 9:20 AM	File folder			
Music	Users		7/18/20	16 2:04 PM	File folder			
Temp	- Wind	ows	4/4/201	7 10:04 AM	File folder			
Videos	Cisco	UserAgent	4/4/201	7 10:28 AM	SQL Server Compact Edition Database File		212 KB	
This PC	N	Scan with Windows Defender		05 8:39 PM	Application extension		874 KB	
Dedter	🗐 t	Open with		16 7:02 PM	Text Document		1 KB	
Desktop	U	Scan for threats						
Documents	-	Sourcefire						
Downloads		Postore province versions						
Music	_	Restore previous versions						
Pictures		Send to	>					
Videos		Cut						
SDisk (C:)		Сору						
🛖 Shared Folders (_	Create shortcut						
A Network	•	Delete						
11 items 1 item selected 2	12 КВ 🚺	Rename						

Passo 6: Volte para services.msc. Clique com o botão direito do mouse no serviço Cisco User Agent, selecione **Properties**, selecione a guia **Log On** e configure um usuário como um login de usuário do AD. Clique em **Apply** quando terminar.

Services				- 🗆	\times
File Action View H	Help				
File Action View H File Action View H Services (Local) C A D P fr ret to	Help Cisco Firepower User Agent for Active Directory Properties (Local C × General Log On Recovery Dependencies Log on as:	cription litates t /ides su :esses in /ides inf lia Man omatica omatica sfers fil dows in Base Fil	Status Running Running Running Running Running Running	Startup Type Manual (Trig Manual Manual Manual Automatic Disabled Automatic (D Automatic Automatic Manual	Log ^ Loc Loc Loc Loc Loc Loc Loc Loc Loc Loc
	OK Cancel Apply	SVC hos WBENG bles wir Bluetoo service ies user o AnyC s netwo bles Cis bles Cis vides inf	Running Running Running Running 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

Passo 7: No services.msc, clique em Start para o Cisco Firepower User Agent para o serviço Ative Diretory.

🌼 Services					- 🗆	×
File Action View	Help					
⇐ ➡ 📰 🖾	à 📑 🚺 📷 🕨 💷 II ID					
🔍 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
	Description: 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
		🌼 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 🗸
		<				>
	Extended Standard					

Passo 8: Verifique o tamanho do arquivo UserAgentEncryptionBytes.bin. Não deve ser 0 KB.

→ * 个 🏪 > This	PC > OSDisk (C:)			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			
Dicturer		10/30/2015 3:24 AM	File folder			
Dealters 7	Program Files	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	隌 CiscoUserAgent	4/4/2017 10:36 AM	SQL Server Compact Edition Database File	2	I2 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 (\\vr						

Etapa 9: Adicione os Controladores de Domínio e o Firepower Management Center ao User Agent Client. Certifique-se de adicionar os Controladores de domínio/host local antes de adicionar o Firepower Management Center ao Agente de usuário.

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

Referências

- Guia de Configuração do Agente de Usuário do Firepower, 2.3
- <u>O agente de usuário pára de derivar se não conseguir converter a conta de serviço em</u> <u>SecurityIdentifier (CSCuw20184)</u>
- <u>Conceder permissão mínima para uma conta de usuário do Ative Diretory usada pelo agente</u> de usuário da Sourcefire